SCSIport Miniport Driver

Version 5.30a2 and Later

for Windows Server 2003 and Windows 2000 Server

User Manual

Copyright© 2007 Emulex Corporation. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Emulex Corporation.

Information furnished by Emulex Corporation is believed to be accurate and reliable. However, no responsibility is assumed by Emulex Corporation for its use; or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of Emulex Corporation.

Emulex, AutoPilot Installer, BlockGuard, cLAN, FabricStream, FibreSpy, Giganet, HBAnyware, InSpeed, IntraLink, LightPulse, MultiPulse, SAN Insite, SBOD and Vixel are registered trademarks, and AutoPilot Manager, EZPilot, SLI and VMPilot are trademarks, of Emulex Corporation. All other brand or product names referenced herein are trademarks or registered trademarks of their respective companies or organizations.

Emulex provides this manual "as is" without any warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Emulex Corporation may make improvements and changes to the product described in this manual at any time and without any notice. Emulex Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties that may result. Periodic changes are made to information contained herein; although these changes will be incorporated into new editions of this manual, Emulex Corporation disclaims any undertaking to give notice of such changes.

.

Installation 1

Introduction 1
Important Considerations 2
Changing Driver Types 2
Updating the SCSIport Miniport Driver Using AutoPilot Installer 2
Upgrading from Windows 2000 Server to Windows Server 2003 2
Definitions 2
SCSIport Miniport Driver Information 3
Prerequisites 3
Compatibility 3
New in This Release 3
Known Issues 3
Things to Know 4
Files Included in this AutoPilot Installer 5
Distribution Executable File Overview 6
Running the Distribution Executable File 6
AutoPilot Installer 7
Introduction 7
Prerequisites 7
AutoPilot Installer Features 7
Configuration Questions 7
Installation Planning 7
AutoPilot Installation Procedures 8
Hardware-First Installation 8
If the Installation Fails 9
Software-First Installation 9
Installing the HBAnyware Security Configurator 10
Unattended Installation 11
AutoPilot Configuration File Format 11
Mandatory Configuration File Changes 11
Deleting Questions in the APInstall.cfg File 12
Optional Configuration File Changes 12
Setting Up Driver Parameters 15
Setting Up System Parameters 15
Unattended Error Codes Reference Table 15
Invoking AutoPilot Installer 16
Batch File Example 16
Manually Installing or Updating the SCSIport Miniport Driver 18
Overview 18
Manually Installing or Updating the Emulex PLUS (ElxPlus) Driver 18
Manually Installing or Updating the SCSIport Miniport Driver 19
Manually Installing the Driver Utilities 20
Uninstalling the Utility Package 20
Uninstalling the Emulex Drivers 22
Installing the Emulex Simulate Device 22

Configuration 23

Introduction 23
Starting HBAnyware from the Desktop 24

Changing Management Mode 25
Starting the HBAnyware Security Configurator 26
Starting HBAnyware from the Command Line 27
HBAnyware Window Element Definitions 28
The Menu Bar 28
The Toolbar 28
The Toolbar Buttons 28
Discovery-Tree 29
Property Tabs 30
Status Bar 30
Using the HBAnyware Command-Line Interface 30
The CLI Client Command Reference 32
Starting the LightPulse Utility (lputilnt) 48
lputilnt Category Summaries 48
Discovering HBAs 49
Discovering HBAs with HBAnyware 49
Configuring Discovery Settings 49
Discovering HBAs Using lputilnt 50
Resetting the HBA 51
Resetting the HBA with HBAnyware 51
Resetting the HBA with lputilnt 51
Sorting HBA Information 52
Sorting HBAs with HBAnyware 52
Sorting by Host Name 52
Sorting by Fabric Address 52
Sorting Local HBAs Only with HBAnyware 52
Sorting Local HBAs with lputilnt 53
Downloading PCI Configuration Files with lputilnt 53
Viewing HBA Information Using HBAnyware 53
Viewing Discovered Information 53
Viewing Host Information 54
The Host Information Tab 54
The Host Driver Parameters Tab 55
Viewing General HBA Information 56
View Detailed HBA Information 57
Port Attributes Field Definitions 58
Loop Map Table Definitions 58
Viewing Fabric Attributes 59
Discovery Information Field Definitions 59
Viewing Target Information 60
Viewing LUN Information 61
Viewing Port Statistics 62
Port Statistics Field Definitions 62
Viewing Firmware Information 64
Viewing Target Mapping 65
Viewing Driver Parameters 66
Viewing Driver Parameters for an HBA 66
Viewing Driver Parameters for All HBAs in a Host 67
Setting Driver Parameters 69
Activation Requirements 69
Setting Host Parameters Using HBAnyware 69

Setting Driver Parameters for a Host 70
Restoring All Parameters to their Earlier Values 70
Resetting Host Parameters 70
Setting HBA Driver Parameters Using HBAnyware 71
Restoring All Parameters to Their Earlier Values 72
Resetting HBA Parameters 72
Saving HBA Driver Parameters to a File 72
Setting an HBA Parameter Value to the Host Parameter Value 72
Setting Parameters Using lputilnt 73
Resetting HBA Values 74
Driver Parameter Reference Table 75
EmulexOption Detail 85
SCSI Address Map 86
I/O Coalescing 91
Setting Topology 92
Topology Reference Table 92
Setting Topology with HBAnyware 93
Setting Topology with lputilnt 93
Mapping and Masking 94
Automapping SCSI Devices 94
Automapping SCSI Devices with HBAnyware 94
Automapping SCSI Devices with lputilnt 94
Target and LUN Mapping and Masking Using lputilnt 95
Overviews 95
Mapping and Masking Window Defaults 96
Setting Mapping and Masking 96
Globally Automapping All Targets 96
Globally Mapping All LUNs 97
Globally Unmasking or Masking All LUNs 97
Automapping LUNs for a Target 97
Setting Up Persistent Binding 98
Setting Up Persistent Binding with HBAnyware 98
Setting Up Persistent Binding with lputilnt 100
Updating Firmware or Boot Code 102
Updating Firmware or Boot Code with HBAnyware 102
Updating Firmware or Boot Code (Batch Mode) with HBAnyware 105
Updating Firmware or Boot Code with lputilnt 107
Performing Basic Diagnostic Tests with HBAnyware 108
Running a Quick Test 108
Running a POST Test 109
Using Beaconing 110
Starting a Diagnostic Dump 110
Displaying PCI Registers and Wakeup Information 111
Running Advanced Diagnostic Tests with HBAnyware 111
Running Loopback Tests 112
Running End-to-End (ECHO) Tests 114
Saving the Log File 115
Out-of-Band SAN Management 116
Adding a Single Host 116
Adding a Range of Hosts 117

Removing Hosts 118
HBAnyware Security 119
Introduction 119
Starting the HBAnyware Security Configurator 119
Running the Security Configurator for the First Time/Create the ACG 120
Designating a Master Security Client 121
Setting Up and Maintaining Access Control Groups 121
Introduction 121
Selecting/Deselecting Access Control Group Tab on the MSC 121
Viewing the Access Control Group Tab on a Non-MSC 122
ACG Icons 123
Running the Configurator for the First Time/Creating the ACG 123
Adding a Server to the ACG 123
Deleting a Server from the ACG 124
Removing Security from All Servers in the ACG 124
Generating New Security Keys 124
Restoring the ACG to Its Last Saved Configuration 124
Accessing a Switch 125
Setting Up and Maintaining Access Sub-Groups 125
Introduction 125
ASG Icons 126
Creating an ASG 126
Reserved Indices - Examples 127
Adding a Server to an ASG 128
Deleting an ASG 128
Restoring an ASG to Its Last Saved Configuration 128
Editing an ASG 128
About Offline ASGs 130
Backup Masters 130
Introduction 130
Backup Master Eligible Systems 131
Backup Master Tab and Controls 131
Creating a Backup Master 132
Reassigning a Backup Master as the New MSC from the Old MSC 132
Reassigning the New MSC from the Backup Master 133

Troubleshooting 134

Introduction 134
Event Tracing (Windows Server 2003, SP1 only) 134
Event Trace Messages 134
ELS Log Messages (0101 - 0117) 134
Discovery Log Messages (0201 - 0246) 136
Mailbox Log Messages (0310 - 0326) 138
INIT Log Messages (0413 - 0460) 139
FCP Log Messages (0700 - 0737) 141
Node Log Message (0900) 143
Link Log Messages (1301 - 1307) 143
Error Log 144
Viewing the Error Log 144
Event Log Tables 145
Troubleshooting Topics 149
General Situations 149

Security Configurator Situations - Access Control Group (ACG) 150
Security Configurator Situations - Access Sub-Groups (ASG)..... 151
Security Configurator Situations - Backup Masters 152
Security Configurator Situations - Error Messages..... 153
Security Configurator Situations - Master Security Client (MSC)..... 154
Non-Hierarchical and Hierarchical ASG 155

Installation

Introduction

AutoPilot Installer™ for Emulex® SCSIport Miniport drivers provides installation options that range from a simple installation with a few mouse clicks to custom unattended installations that use predefined script files.

AutoPilot Installer is included with Emulex drivers and utilities in Windows executable files that you can download from the Emulex Web site. Run the distribution executable file to extract all of the software needed for an installation, then complete the installation using AutoPilot Installer. AutoPilot Installer allows you to install a driver by any of the following methods:

Hardware-first installation. The host bus adapter (HBA) has already been installed before you download the Emulex drivers and utilities.

Software-first installation. This installation method allows you to download drivers and utilities from the Emulex Web site and to install them using AutoPilot Installer prior to the installation of any HBAs. You do not need to specify the model of the HBA you plan to install. The appropriate drivers and utilities automatically load when you install HBAs at a later time.

Unattended installation. This installation method allows you to set up AutoPilot Installer to run unattended from customized scripts. Unattended installation works for both hardware-first and software-first installations. An unattended installation:

- Enables you to set up one location that contains the distribution executable file. All of the servers install or update the driver and utilities from that location.
- Operates from the command line.
- Operates in silent mode.
- Creates an extensive report file.
- Reports any errors.

Replicated installation. This installation method allows you to preload drivers and utilities on a system. Possible applications include installing a driver and utilities in advance on a system before adding HBAs, and performing system installations that execute AutoPilot Installer in unattended mode.

Important Considerations

Changing Driver Types

- If you currently use a driver type different from the one you will install with AutoPilot Installer you will lose your customized driver parameters, persistent bindings, LUN masking and LUN mapping when you change driver types. The AutoPilot Installer™ default parameters will usually be the best options for the new driver type. You may want to note your current settings before you install the new driver type. After you have installed the new driver type, you can then update your customized driver parameters.

Updating the SCSIport Miniport Driver Using AutoPilot Installer

- If you currently have an older version of the SCSIport Miniport driver (version 5.20ax or older), use the Hardware-first installation method to update your driver. Steps 1 and 2 involve installing a new HBA, therefore begin at step 3 to update the driver.
- You can also update the SCSIport Miniport driver by the manual installation method. If you update the SCSIport Miniport driver manually, install the elxplus driver prior to updating the SCSIport Miniport driver. See “Manually Installing or Updating the SCSIport Miniport Driver” on page 18 for more information.

Upgrading from Windows 2000 Server to Windows Server 2003

- If you are upgrading from Windows 2000 Server to Windows Server 2003 and are currently running an Emulex SCSIport Miniport driver, you must uninstall the driver before upgrading the operating system. Reinstall the SCSIport Miniport driver after you upgrade the operating system.

Definitions

Driver. A host computer software component that controls the operation of peripheral controllers or HBAs attached to the host computer. Drivers manage communication and data transfer between applications and I/O devices, using HBAs as agents.

The HBAnyware™utility (HBAnyware). This utility allows you to perform installation and configuration tasks on remote and local HBAs.

Security Configurator. The HBAnyware security package allows you to control which HBAnyware systems can remotely access and manage HBAs on other systems in a Fibre Channel (FC) network. See page 10 for the installation procedure.

LightPulse® utility (lputilnt). This driver-specific utility for the Storport Miniport and SCSIport Miniport drivers provides a user-friendly interface that allows you to examine, manage and configure installed HBAs. lputilnt is automatically installed when you install the HBAnyware utility.

SCSIport Miniport Driver Information

Prerequisites

One of the following operating systems:

- Windows Server 2003 running on an x86 or Itanium 64-bit platform.
- Windows 2000 Server (Service Pack 4 is recommended).

Note: If you are running Windows 2000 Server with Service Pack 2, the NO_STOPREQ parameter in the EmulexOption must be disabled (it is enabled by default). Perform this task after you have installed the SCSIport Miniport driver and the driver utilities

Compatibility

The Emulex SCSIport Miniport driver is compatible with the following FC HBAs:

- LPe11002, LPe11000 and LPe1150 (minimum firmware version 2.50a2)
- LP11002, LP11000 and LP1150 (minimum firmware version 2.10a5)
- LP10000ExDC and LP1050Ex (minimum firmware version 1.90a4)
- LP10000DC and LP10000 (minimum firmware version 1.80a2)
- LP1005DC-CM2 (minimum firmware 1.90a5)
- LP1050 and LP1050DC (minimum firmware version 1.80a3)
- LP9802DC, LP9802 and LP982 (minimum firmware version 1.00a4)
- LP9402DC, LP9002DC, LP9002L, LP9000 & LP952L (recommended firmware version 3.90a7)
- LP8000, LP8000DC and LP850
    - If your HBA has a Dragonfly chip version 2.00 or greater, use firmware version 3.90a7.
    - If your HBA has a Dragonfly chip below version 2.00, use firmware version 3.30a.

Note: Refer to LP8000 and LP8000DC Firmware Downloads page on the Emulex Web site to determine the Dragonfly chip version in use.

- For all x86 BootBIOS versions (minimum x86 BootBIOS version 1.60)
- EFIBoot Version 3.00a9 or higher (64-bit only)

New in This Release

- The Emulex PLUS (ElxPlus) driver is new in this release. This driver supports HBAnyware, persistent binding and LUN mapping and masking. If you use AutoPilot Installer, this driver is automatically installed before the SCSIport Miniport driver.
- Event trace log messages are new in this release. See the Troubleshooting section for more information.

Known Issues

- If there are multiple HBAs in one system, a reboot is required if a new driver is installed on one or more of the HBAs. A Windows 2000 Server issue will cause the driver to appear as if it has updated successfully, but the old version of the driver will still be running until the system is rebooted.

Things to Know

- Windows support configuring the number of outstanding SCSI requests per SCSI bus. The default is 150 SCSI requests per SCSI bus. Use regedt32 to change the number of requests.
- Windows SCSI subsystems allow the disk I/O time-out value to be increased in case of frequent device I/O time-outs. The default is 60 seconds.
- Adding an HBA to a system while HBAnyware is running causes HBAnyware to freeze. To add an HBA while the system is running (commonly called a hot plug), you must exit the HBAnyware GUI client, insert the HBA, and then re-launch HBAnyware
- Some Web browsers will continuously try to reload the HBAnyware online help making it unusable. In this case, disable the Web browser's JavaScript capabilities. Refer to the Web browser's help for more information.

Files Included in this AutoPilot Installer

The Distribution File copies the AutoPilot Installer Files to your system. By default, these files are copied to c:\\Program Files\Emulex\AutoPilot Installer.

Table 1: AutoPilot Installer Files

Folder	Description
AutoPilot Installer	This folder contains the following files necessary to run the AutoPilot Installer: • APInstall.exe - Executable file for the AutoPilot Installer. • APInstall.cfg - Configuration file for the AutoPilot Installer. • FriendlyName.exe - Provides display names for installed HBAs.
ApInstaller_IA64 Folder ApInstaller_x86 Folder	These folders contain the following files necessary to run the AutoPilot Installer: • APInstall.exe - Executable file for the AutoPilot Installer. • APInstall.cfg - Configuration file for the AutoPilot Installer. • SilentApInstallIExampleText.txt - Information and example script for silent installations.
Drivers Folder	This folder contains the SCSIport Miniport folder and all files necessary to install the driver. Separate folders for each architecture (x86 and Itanium 64-bit) contain these following files: • txtsetup.oem - Driver installation script for boot-time setup program (BootBIOS must be installed). • lpxnds.sys - SCSIport Miniport driver • elxplus - A non-filter driver. This new driver supports HBAnyware, persistent bindings and LUN mapping and masking. • lpscsi - File used for F6 installation • lpxnds.dll - co-installer • lpsimdev.inf - Installation script of Emulex Simulate Device • lpxnds.cat - Miniport driver catalog file • lpsimdev - Emulex Simulate Device Catalog file
Utilities	This folder contains files necessary to install HBAnyware and the driver utility: The setupapps.exe installs utilities and related files which include: LightPulse utility (lputilnt) HBAnyware HBAnyware Discovery Server
Reports	If the system generates reports, this folder is generated and the reports are placed here.

Distribution Executable File Overview

The distribution executable file self-extracts and copies the following onto your system:

- AutoPilot Installer
- SCSIport Miniport driver
- HBAnyware utility
- HBAnyware Security Configurator
- LightPulse utility (lputilnt)

After the distribution executable file runs and the files are extracted, you have two options:

- Run AutoPilot Installer immediately
- Run AutoPilot Installer later

Running the Distribution Executable File

To run the distribution executable file:

1. Download the distribution executable file from the Emulex Web site to your system.
2. Double-click the distribution executable file. A window is displayed with driver version information and Emulex contact information.
3. Click **Next** to access the Installation Folder window or click **Cancel** to close the window.
4. The default installation location is displayed. Browse to a different location, if desired. Click **Install** to continue the installation.
5. The Progress window is displayed. As each task completes, the corresponding box is automatically selected.
6. After all tasks complete, a confirmation window is displayed. The Start AutoPilot Installer box is automatically selected. To start AutoPilot Installer later, clear this box.
7. Click **Finish** to close the distribution executable file.

AutoPilot Installer

Introduction

The Emulex AutoPilot Installer is a Fibre Channel HBA installation wizard for Windows. The AutoPilot Installer installs (or updates) Emulex drivers and utilities and configures HBAs, drivers and utilities.

Prerequisites

One of the following operating systems:

- Windows Server 2003 running on an x86 or Itanium 64-bit platform.
- Windows 2000 Server (Service Pack 4 is recommended).

Note: If you are running Windows 2000 with Service Pack 2, the NO_STOPREQ parameter in the EmulexOption must be disabled (it is enabled by default). Perform this task after you have installed the SCSIport Miniport driver and the driver utilities.

AutoPilot Installer Features

- Command line functionality - invokes AutoPilot Installer from the command line using customized installation scripts
- Driver and utility updates - installs and updates drivers and utilities
- Multiple HBA installation capability - installs drivers on multiple HBAs, alleviates the need to manually install the same driver on all HBAs in the system
- Driver diagnostics - determines whether the driver is properly operating
- Silent installation mode - suppresses all screen output (necessary for unattended installation)

Configuration Questions

Vendor-specific versions of the Emulex driver installation program may include one or more windows with questions that you must answer before continuing the installation process.

Installation Planning

Table 2 describes the types of installations that you can perform under certain conditions. Use this information to determine which method to use for your situation.

Table 2: Types of Installations

	Attended Installations		Unattended Installations	
Condition	**Hardware-First Installation**	**Software-First Installation**	**Unattended Installation**	**Replicated Installation**
No HBA in a single system		X	X	X
New HBA in a single system	X		X	X
Existing HBAs and drivers installed, updated driver available	X		X	X
Multiple systems, no HBAs installed		X	X	X
Multiple systems, new HBAs installed	X		X	X

AutoPilot Installation Procedures

Hardware-First Installation

Prerequisites

- The Distribution Executable file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.

Note: To update the SCSIport Miniport driver, begin the following procedure at step 2.

Procedure

To perform a hardware-first installation:

1. Install a new Emulex HBA and power-on the system. If the Windows Found New Hardware wizard is displayed, click **Cancel** to exit. AutoPilot Installer performs this function.

Note: If there are multiple HBAs in the system, the Windows Found New Hardware wizard appears for each HBA. Click **Cancel** to exit the wizard for each HBA.

2. If you have already extracted the driver and utility files, run the APInstaller.exe file.

   If you have not extracted the driver and utility files, run the distribution executable file (see “Running the Distribution Executable File” on page 6) and leave the Start AutoPilot Installer box selected. Click **Finish**.
3. Click **Next**. Installation automatically completes, except in the following situations:
   - If you are changing driver types, the Available Drivers window appears. This window allows you to select a new driver type. Select the driver type from the drop-down list and click **Next**.
   - If you are installing an older driver version, the Available Drivers window is displayed. Select the existing driver version from the drop-down list and click **Next**.
   - If you are installing a vendor-specific version of the Emulex driver installation program, this program may include one or more windows with questions that you must answer before continuing the installation process. In this case, answer each question and click **Next** on each window to continue.
4. View the progress of the installation. Once the installation is successful, a congratulations window appears.
5. View or print a report, if desired.
   - View Installation Report - your text editor (typically Notepad) shows a report with current HBA inventory and configuration information and task results. The text file is named in the following format: *report_MM-DD-YY-#*.txt
     - *MM* = month
     - *DD* = day
     - *YY* = year
     - # = report number
   - Print Installation Report - your default print window is displayed.
6. Click **Finish** to close AutoPilot Installer. If your system requires a reboot, you are prompted to do so when you click **Finish**.

If the Installation Fails

If the installation fails, the Diagnostics window appears. To view the reason an HBA failed, select the HBA row. The reason and suggested corrective action are displayed below the list.

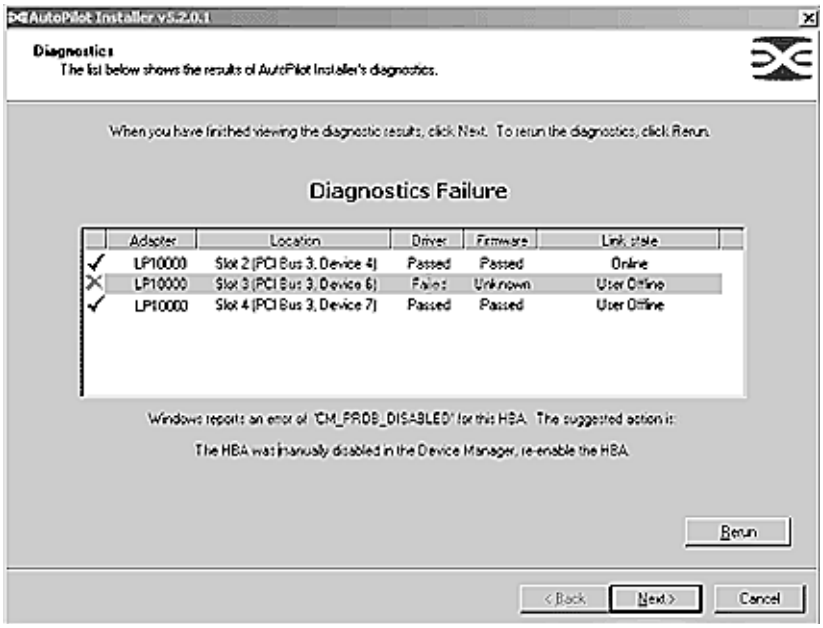

Figure 1: AutoPilot Installer, Diagnostics Window (Example)

Perform the suggested corrective action and run APInstaller.exe again.

Software-First Installation

Prerequisites

- The Distribution Executable file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.

Procedure

To perform a software-first installation:

1. If you have already extracted the driver and utility files, run the APInstaller.exe file.

   If you have not extracted the driver and utility files, run the distribution executable file (see page 6), and leave the Start AutoPilot Installer box selected. Click **Finish**.

   The following message appears:

AutoPilot Installer Warning
AutoPilot Installer cannot find any Emulex Fibre Channel HBAs in this system.
AutoPilot Installer can perform a driver pre-installation, allowing you to install your HBAs later.
Click OK to pre-install drivers, or click Cancel to stop the installation.
OK
Cancel

Figure 2: AutoPilot Installer Message (Software-First Installation)

2. Click **OK**.
3. The welcome window appears.
4. Click **Next**. Installation automatically completes.
5. View the progress of the installation. Once the installation is successful, a congratulations window appears.
6. View or print a report, if desired.

   View Installation Report - your text editor (typically Notepad) displays a report with task results. The text file is named in the following format: *report_MM-DD-YY-#*.txt

   - *MM* = month
   - *DD* = day
   - *YY* = year
   - # = report number

   Print Installation Report - your default print window is displayed.
7. Click **Finish** to close AutoPilot Installer. If the system needs to reboot, you are prompted to do so when you click **Finish**.

Installing the HBAnyware Security Configurator

After the HBAnyware utility and remote server are installed on a group of systems, HBAnyware can remotely access and manage the HBAs on any systems in the group. This may not be desirable because any system with remote access can perform actions such as resetting boards or downloading firmware.

The HBAnyware Security Configurator controls which HBAnyware systems can remotely access and manage HBAs on other systems in an FC network. HBAnyware security is system-based, not user-based. As a result, anyone who can access a system with HBAnyware client access to remote HBAs can manage those HBAs.

Prerequisites

- The SCSIport Miniport driver is properly installed.
- The HBAnyware and lputilnt utilities are properly installed.

Procedure

To install the HBAnyware Security Configurator:

1. Locate the SSCsetup.exe file. The default path for this file is:

   `C:\Program Files\HBAnyware`
2. Double-click the SSCsetup.exe file. A welcome window appears. Click **Next**.
3. The Setup Status window is displayed. After setup completes, the Emulex HBAnyware Security Setup Completed window appears.
4. Click **Finish**.

Unattended Installation

Unattended installation is invoked from the command line. The apinstall command uses installation and driver settings stored in a configuration file (APInstall.cfg). The default APInstall.cfg file is located in the AutoPilot Installer folder in the Emulex folder in the Program Files directory.

Make a copy of the APInstall.cfg file before you make modifications. The APInstall.cfg file should be used as a starting point for scripting an unattended installation.

You must modify the APInstall.cfg file to enable silent mode, specify a driver location and specify allowable driver types.

You can change the installation report name and location from the default, as well as enable optional parameters.

Prerequisites

- The Distribution Executable file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.
- It is highly recommended that you make a copy of the APInstall.cfg file and rename it for your customization.

AutoPilot Configuration File Format

The APInstall.cfg file is organized into commented sections, grouped according to related commands.

- Lines that begin with a semicolon are comments. To enable sample comment lines, remove the semicolon.
- There are four main sections. Two are required and two are optional. Driver parameters must be set up in the [SCSIPORT.PARAMS] section. Each section begins with a heading.
  - [AUTOPILOT.CONFIG] - this required section contains settings that control and configure the AutoPilot Installer's operation.
  - [SCSIPORT.CONFIGURATION] - this optional section may contain questions that must be answered during the installation process. This section applies to attended installations only.
  - [SCSIPORT.PARAMS] - this required section can specify driver parameters. Parameters are read exactly as they are entered and are written to the registry.
  - [SYSTEM.PARAMS] - this section may be created to specify system parameters.

Mandatory Configuration File Changes

Locate the Mandatory Configuration File Changes heading in the [AUTOPILOT.CONFIG] section of the APInstall.cfg file.

Enabling Silent Mode

You may enable silent mode to run an unattended installation. To enable silent mode, remove the semicolon before:

```
;SilentInstallEnable = "TRUE"
```

Setting Up Allowable Driver Types

Four configuration file settings determine what driver types the AutoPilot Installer can install. Remove the semicolon before:

```
;win2000DriverPreference = "SCSIPORT"
;win2003DriverPreference = "SCSIPORT"
;win2000AllowableDrivers = "SCSIPORT"
;win2003AllowableDrivers = "SCSIPORT"
```

Note: All four of these settings must specify the same driver type.

Setting Up Driver Location

When in silent mode, you need to specify the location of the driver to be installed. Locate the following line in the APInstall.cfg file:

```
;LocalDriverLocation = "C:\Path\toThe\SCSIPortDriver\Package"
```

Remove the semicolon before this line and modify this path to reflect the location of the driver.

The driver location can be a local disk or a network shared drive. It can also be a relative path to the apinstall.cfg file. The location must be specific to the x86 or IA64 folder to install the correct driver for the server platform.

Full path example for an x86 driver (all on one line):

```
LocalDriverLocation = “C:\Program Files\Emulex\AutoPilot Installer\Drivers\SCSIport Miniport\x86”
```

Relative path example for Itanium 64-bit driver:

```
LocalDriverLocation = “Drivers\SCSIport Miniport\IA64”
```

Deleting Questions in the APInstall.cfg File

A [SCSIPORT.CONFIGURATION] section may exist in the APInstall.cfg file. If this section does exist, it may contain a [QUESTIONS] section with vendor-specific installation questions. You must remove the entire [SCSIPORT.CONFIGURATION] section or comment it out for a silent installation.

Optional Configuration File Changes

Locate the Optional Configuration File Changes heading in the [AUTOPILOT.CONFIG] section of the APInstall.cfg file. This heading follows Mandatory Configuration File Changes.

Changing Utility Installation Location

AutoPilot Installer normally installs utilities from a Utilities subdirectory located in the same directory as AutoPilot Installer.

To modify the location, locate the following in the APInstall.cfg file (all in one line):

```
; UtilitiesLocation = "C:\Program Files\Emulex\Autopilot Installer\Windows\Utilities"
```

Remove the semicolon before this line and modify this directory path to specify an alternate location, such as a network shared drive.

Setting Up an Automatic System Restart During an Unattended Installation

AutoPilot Installer does not automatically perform system restarts for the following reasons:

- Restarts often require a login as part of Windows start-up process. If the system is restarted, the installation process stops until a login is performed.
- AutoPilot Installer does not know if it is safe to restart the system. Restarts while applications are active can result in the loss of data.

To configure Windows to start up without requiring a login, remove the semicolon from this line:

```
; SilentRebootEnable = "FALSE"
```

Change this parameter to true:

```
SilentRebootEnable = "TRUE"
```

Setting Up Installation Report Title and Location

You can change the Installation report name and the location to which it is written. This information must be specified in one command. In the following example x is the system drive. Remove the semicolon before:

```
; ReportLocation = "x: \autopilot\reports\installs\March16-06.txt"
```

Default File Name

This default file name format is ”report_mm-dd-yy.txt” and uses ‘mm’ for the month, ‘dd’ for the date, and ‘yy’ for the year.

Default Report Location

By default, the report is written to the system drive. In the following example x is the system drive. Your system drive may be different. You can modify this line to change the report location and/or file name.

```
" ReportLocation =  "x: \autopilot\reports\installs\March16-06.txt"
```

Note: Both the report location and file name must be specified.

Setting Up an Installation Without Utilities

You can set up the unattended installation to install the driver without installing the utilities package. The default for this setting is false which means that the utilities are automatically installed with an unattended installation. To set up an installation without utilities, remove the semicolon before:

```
; SkipUtilityInstall = "FALSE”
```

Change this parameter to true:

```
SkipUtilityInstall = "TRUE”
```

Setting Up Existing Driver Parameters Retention or Override

The ForceRegUpdate driver parameter setting determines if existing driver parameters are retained or changed when you update the driver. This parameter defaults to False and means all existing driver parameter settings are retained. Setting the ForceRegUpdate parameter to True causes removal of all existing driver parameters from the registry and replaces them with the parameters specified in the APInstall.cfg file. The ForceRegUpdate parameter does not affect any existing persistent bindings.

To set up an installation to remove the existing driver parameters from the registry and replace them with parameters specified in the APInstall.cfg file, remove the semicolon before:

```
;ForceRegUpdate = "FALSE"
```

Note: You can also use this setting for attended installations with the AutoPilot Installer wizard if you modify the APInstall.cfg file in the AutoPilot Installer folder.

Change this parameter to true:

```
ForceRegUpdate = "TRUE"
```

Setting Up Re-Installation of an Existing Driver Version

By default, AutoPilot Installer will only update a driver if the new driver version is different from the installed driver version. If necessary, you can use the ForceDriverUpdate setting to re-install the same driver version. To force a re-installation of the same driver type and version, remove the semicolon from this line:

```
; ForceDriverUpdate = "FALSE"
```

Change this parameter to true:

```
ForceDriverUpdate = "TRUE"
```

Note: This setting can only be used for unattended installations.

Setting Up a Driver Type to Force

By default the ForceDriverTypeChange parameter is set to ‘FALSE’. When set to the default, AutoPilot Installer will install drivers on HBAs that have no other driver installed, or whose current driver type matches that of the driver being installed.

If this parameter is changed to ‘TRUE’, AutoPilot Installer will cause silent installations to update or install the current driver on each HBA in the system, without any regard to driver type. For example, you would want this option left on or set to “TRUE’ to silently install the Storport Miniport driver on any HBAs currently running SCSIport Miniport or FC Port drivers.

Remove the semicolon from this line:

```
;ForceDriverTypeChange = "FALSE"
```

Change this parameter to true:

```
ForceDriverTypeChange = "TRUE"
```

Setting Up Driver Parameters

To change driver parameter defaults, modify this section of the APInstall.cfg file. Locate the [SCSIPORT.PARAMS] section in the APInstall.cfg file. This section follows Optional Configuration File Changes. Under the [SCSIPORT.PARAMS] heading, list the parameters and new values for the driver to use. All driver parameters need to be listed in a single line, separated by a semicolon.

For example, Driver Parameter = “LinkTimeout = 45;NodeTimeout=60;SimulateDevice=1;Topology=2;”

See the “Driver Parameter Reference Table” on page 75 for a listing of driver parameters and their defaults and valid values.

Note: It is necessary to list all driver parameters in a single line for the parameter values to be added to the registry as individual keys.

The “SimulateDevice=1” parameter must be included for the changes to be effective. See the example above.

A discrepancy exists in the APInstall.cfg file. The APInstall.cfg file incorrectly lists driver parameters on separate lines.

Setting Up System Parameters

To change the system parameters, create a [SYSTEM.PARAMS] section in the APInstall.cfg file. Create this section in the Optional Configuration File Changes heading in the [AUTOPILOT.CONFIG] section of the APInstall.cfg file.

Unattended Error Codes Reference Table

AutoPilot Installer sets an exit code to indicate whether an installation was successful or an error occurred. These error codes allow AutoPilot Installer to be used in scripts with error handling. AutoPilot Installer’s silent mode specifically returns the following values:

Table 3: Unattended Installation Error Codes

Error Code	Hex	Description
0	0x00000000	No errors.
2	0x00000002	No appropriate driver found.
87	0x00000087	Invalid configuration file parameters.
110	0x0000006E	Could not open installation report file.
1248	0x000004E0	No HBA found.
2001	0x000007D1	Driver found is the same type as the existing driver and has the same, or older, version number.
2399141889	0x8F000001	Unsupported operating system detected.
2399141890	0x8F000002	AutoPilot could not locate the configuration file.
2399141891	0x8F000003	One or more HBAs is disabled.
2399141892	0x8F000004	The selected driver is 64-bit and this system is 32-bit.
2399141893	0x8F000005	The selected driver is 32-bit and this system is 64-bit.
2399141894	0x8F000006	Other hardware installation activity is pending.

Table 3: Unattended Installation Error Codes (Continued)

Error Code	Hex	Description
2399141895	0x8F000007	The user does not wish to perform a 'software-first' install.
2399141896	0x8F000008	Silent installation did not find any appropriate drivers.
2399141897	0x8F000009	A silent reboot was attempted, but returned an error code instead.

Invoking AutoPilot Installer

If the configuration file has been modified and saved with its original name (APInstall.cfg) and you want to invoke the AutoPilot Installer, at the command line, type:

```
apinstall
```

If the configuration file has been modified and saved with a different name and/or the configuration file location has changed, you must specify the entire path location (using the standard drive:\directory path\filename format) and the entire name of the configuration file. In the following example, the configuration file has been renamed and relocated:

Example:

ApInstall g:\autopilot\mysetup\cs_apinstall.cfg

Batch File Example

Modifying the configuration file enables you to script the installation of a system's driver. The following example batch file assumes that you have made mandatory changes to the APInstall.cfg file, as well as any desired optional changes.

If your systems have been set up with a service that supports remote execution, then you can create a batch file to remotely update drivers for all of the systems on the storage net. If Microsoft's RCMD service was installed, for example, a batch file similar to the following would run remote execution:

```
rcmd \\server1 g:\autopilot\ApInstall g:\autopilot\mysetup\apinstall.cfg
if errorlevel 1 goto server1ok
echo AutoPilot reported an error upgrading Server 1.
if not errorlevel 2147483650 goto unsupported
   echo Configuration file missing.
goto server1ok
 :unsupported
 if not errorlevel 2147483649 goto older
   echo Unsupported operating system detected.
 :older
 if not errorlevel 2001 goto none
   echo The driver found is the same or older than the existing driver.
   goto server1ok
:none
 if not errorlevel 1248 goto noreport
   echo No HBA found.
goto server1ok
:noreport
 if not errorlevel 110 goto nocfg
   echo Could not open installation report file.
 goto server1ok
```

```
:nocfg
 if not errorlevel 87 goto badcfg
   echo Invalid configuration file parameters.
   goto server1ok
:badcfg
   if not errorlevel 2 goto server1ok
   echo No appropriate driver found.
server1ok

rcmd \\server2 g:\autopilot\ApInstall g:\autopilot\mysetup\apinstall.cfg
if errorlevel 1 goto server2ok
echo AutoPilot reported an error upgrading Server 2.
if not errorlevel 2147483650 goto unsupported
   echo Configuration file missing.
goto server2ok
 :unsupported
 if not errorlevel 2147483649 goto older
   echo Unsupported operating system detected.
 :older2
 if not errorlevel 2001 goto none2
   echo The driver found is the same or older than the existing driver.
   goto server2ok
:none2
 if not errorlevel 1248 goto noreport2
   echo No HBA found.
goto server2ok
:noreport
 if not errorlevel 110 goto nocfg2
   echo Could not open installation report file.
 goto server2ok
:nocfg2
 if not errorlevel 87 goto badcfg2
   echo Invalid configuration file parameters.
   goto server2ok
:badcfg2
   if not errorlevel 2 goto server2ok
   echo No appropriate driver found.
server2ok
```

Manually Installing or Updating the SCSIport Miniport Driver

You can install or update the SCSIport Miniport driver and utilities manually without using AutoPilot Installer.

Overview

The Emulex PLUS (ElxPlus) driver is new to this version and supports HBAnyware, persistent binding and LUN mapping and masking. The ElxPlus driver replaces the adjunct driver. The ElxPlus driver must be installed before you install the SCSIport Miniport driver.

The SCSIport Miniport driver and ElxPlus driver were extracted when you ran the Distribution Executable File.

Prerequisites

- The Distribution Executable file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.

Manually Installing or Updating the Emulex PLUS (ElxPlus) Driver

Procedure

To install or update the ElxPlus driver from the desktop:

1. Select Start, Control Panel and Add Hardware. The Add Hardware Wizard window appears.
2. Click **Next**.
3. Select “Yes, I have already connected the hardware”.
4. Click **Next**.
5. Select, “Add a new hardware device”.
6. Click **Next**.
7. Select "Install the hardware that I manually select from a list (Advanced)".
8. Click **Next**.
9. Select “Show All Devices”.
10. Click **Next**.
11. Click **Have Disk...** Direct the Device Wizard to the location of elxplus.inf. If you have downloaded the SCSIport files to the default directory, the path will be:
    - C\Program Files\Emulex\AutoPilot Installer\Drivers\SCSIport\x86 for the 32-bit driver version

    or

    - C\Program Files\Emulex\AutoPilot Installer\Drivers\SCSIport\IA64 for the Itanium 64-bit driver version.
12. Direct the Add Hardware wizard to the location of the driver’s distribution kit (you may need to click **Browse**, find the location and select elxplus.inf).
13. Click **OK**.
14. Select "Emulex PLUS".
15. Click **Next** and click **Next** again to install the driver.
16. The ElxPlus driver installation is complete. Continue with manual installation of the SCSIport Miniport Driver.

Manually Installing or Updating the SCSIport Miniport Driver

Procedure

To update or install the SCSIport Miniport driver from the desktop:

1. Select Start, Control Panel and System.
2. Select the Hardware tab.
3. Click **Device Manager**.
4. Open the "SCSI and RAID Controllers" item.
5. Double-click the desired Emulex HBA.

Note: The driver will affect only the selected HBA. If there are other HBAs in the system, you must repeat this process for each HBA. All DC models will be displayed in Device Manager as two HBAs, therefore each HBA must be updated.

6. Select the **Driver** tab.
7. Click **Update Driver.** The Update Driver wizard starts.
8. Select "Install from a list or specific location (Advanced)". Click **Next**.
9. Select "Don't search. I will choose the driver to install". Click **Next**.
10. Click **Have Disk...** Direct the Device Wizard to the location of oemsetup.inf. If you have downloaded the SCSIport files to the default directory, the path will be:
    - C\Program Files\Emulex\AutoPilot Installer\Drivers\SCSIport\x86 for the 32-bit driver version

    or

    - C\Program Files\Emulex\AutoPilot Installer\Drivers\SCSIport\IA64 for the Itanium 64-bit driver version.
11. Click **OK**.
12. Select "Emulex *LPX000* Fibre Channel SCSIport Driver" (your HBA model will be displayed here).
13. Click **Next**.
14. Click **Finish**.

The driver installation is complete. The driver should start up automatically. If the HBA is connected to a Fibre Channel switch, hub or data storage device, a blinking yellow light on the back of the HBA will indicate a link up condition.

Manually Installing the Driver Utilities

The utility installation installs HBAnyware and lputilnt.

Prerequisites

- The ElxPlus driver is properly installed.
- TheSCSIport Miniport driver is properly installed.
- The Distribution Executable file has been downloaded from the Emulex Web site and extracted to a directory on your local drive. If you have downloaded the SCSIport Miniport files to the default directory, the path will be: C\\Program Files\Emulex\AutoPilot Installer\Utilities\.

Procedure

To install the utility:

1. Run setupapps.exe.
2. Follow the instructions on the setup windows.
3. Click **Finish** in the last dialog box to exit Setup. The utility installation has completed.The HBAnyware utility automatically starts running.

Uninstalling the Utility Package

To uninstall the HBAnyware utility package:

1. Click Start, Settings, and Control Panel. The Add/Remove Programs window appears. Select the Install/Uninstall tab. A window similar to Figure 3 appears:

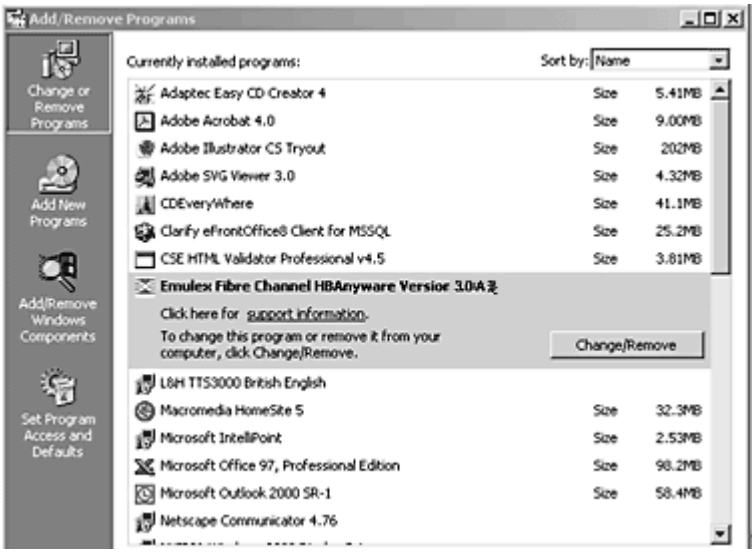
Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Currently installed programs:
Sort by: Name
Adaptec Easy CD Creator 4 Size 5.41MB
Adobe Acrobat 4.0 Size 9.00MB
Adobe Illustrator CS Tryout Size 202MB
Adobe SVG Viewer 3.0 Size 4.32MB
CDEveryWhere Size 41.1MB
Clarify eFrontOffice8 Client for MSSQL Size 25.2MB
CSE HTML Validator Professional v4.5 Size 3.81MB
Emulex Fibre Channel HBAnyware Version 3.0A3
Click here for support information.
To change this program or remove it from your computer, click Change/Remove.
Change/Remove
L&H TTS3000 British English
Macromedia HomeSite 5 Size 32.3MB
Microsoft IntelliPoint Size 2.53MB
Microsoft Office 97, Professional Edition Size 98.2MB
Microsoft Outlook 2000 SR-1 Size 58.4MB
Netscape Communicator 4.76

Figure 3: Add Remove Programs Window

2. Select the Emulex Fibre Channel item and click **Change/Remove**. A window similar to Figure 4 appears:

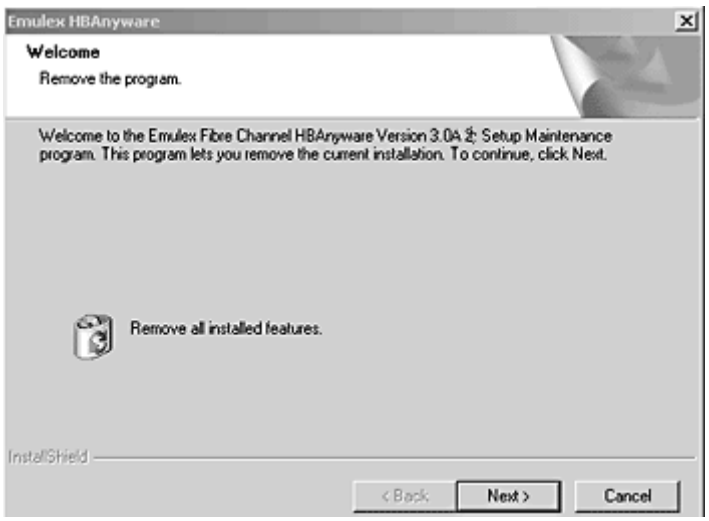
Emulex HBAnyware
Welcome
Remove the program.
Welcome to the Emulex Fibre Channel HBAnyware Version 3.0A Setup Maintenance program. This program lets you remove the current installation. To continue, click Next.
Remove all installed features.
InstallShield
< Back
Next >
Cancel

Figure 4: Emulex HBAnyware Welcome Window

3. Click **Next**. The utilities are removed from the system.

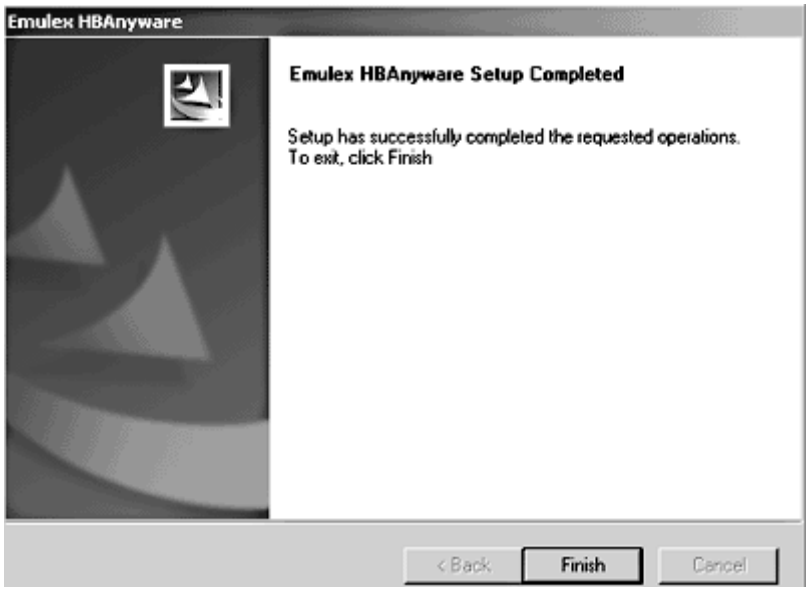

Figure 5: Emulex HBAnyware Completion Window

4. Click **Finish**. Uninstallation is complete.

Uninstalling the Emulex Drivers

The Emulex SCSIport Miniport and Emulex PLUS (ElxPlus) drivers are uninstalled using the Device Manager.

Prerequisites

- The Distribution Executable file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.

Procedures

To uninstall the Emulex SCSIport driver:

1. Select Start, All Programs, Administrative Tools and Computer Management.
2. Click **Device Manager**.
3. Double-click the HBA from which you want to remove the SCSIport Miniport driver. A device-specific dialog box is displayed. Click the **Driver** tab.
4. Click **Uninstall** and click **OK** to uninstall.

To uninstall the ElxPlus driver (uninstall the ElxPlus driver only if all HBAs and installations of Emulex miniport drivers are uninstalled).

After running Device Manager (steps 1 and 2 above):

1. Click the plus sign (+) next to the Emulex PLUS driver class.
2. Right-click the Emulex driver and click **Uninstall**.
3. Click **OK** in the Confirm Device Removal Window.

Installing the Emulex Simulate Device

Installing the Emulex Simulate Device creates a dummy disk to force the driver to load if no disk devices are present at boot time. The Emulex Simulate Device is enabled by setting the SimulateDevice parameter to 1 (it is disabled by default). You can enable this setting using the lputilnt.

Note: Microsoft provides simulate device (CreateInitiatorLU) functionality on Windows Server 2003 and it is enabled by default during installation of the Emulex SCSIport Miniport driver. If you have a Windows Server 2003 system, use the simulate device provided by Microsoft.

To install the Emulex simulate device:

1. Restart the computer. A "Found New Hardware Wizard" window appears. Click Next.
2. Select "Display a list of known drivers for this device so that I can choose a specific driver", and click Next.
3. Select "System Devices" and click Next.
4. Select "Emulex" in the Manufacturers window. Select "Emulex Simulate Device" in the Models window. Click Next.
5. Follow the instructions to finish installing this device.

Configuration

Introduction

The Emulex®SCSIport Miniport has many options that you can modify to provide for different behavior. You can change these options in one of two ways:

- The HBAnyware™ utility (HBAnyware) is a user-friendly graphical environment. Use HBAnyware to do any of the following:
    - Discover local and remote hosts, host bus adapters (HBAs), targets and LUNs
    - Reset HBAs
    - Set up persistent binding
    - Set HBA driver parameters
    - Set driver parameters simultaneously to multiple HBAs using Batch Update
    - Set global driver parameters to HBAs
    - Update firmware on the single HBA or multiple HBAs using Batch Update
    - Enable boot code
    - Run diagnostic tests on HBAs
    - Manage out-of-band HBAs
    - Manage local and in-band remote HBAs
    - Update EFIBoot (64-bit only)

Note: HBAnyware can only discover and manage remote HBAs on hosts running HBAnyware's elxhbamgr. For in-band management, remote capabilities of HBAnyware are subject to fabric zoning configuration. Remote hosts you want to discover and manage by HBAnyware must be in the same zone.

- The LightPulse™ utility (lputilnt) allows you to set driver parameters on local HBAs only. Use lputilnt to do any of following:
    - Download Peripheral Component Interconnect (PCI) configuration data files
    - Assign an Arbitrated Loop Physical Address (AL_PA)
    - Perform global and target mapping and masking
    - Globally automap all logical unit numbers (LUNs)
    - Globally unmask all LUNs
    - Set up persistent binding
    - Hot swap a device
    - Set topology options
    - Map device identifiers (IDs)
    - Break SCSI reservations
    - Set driver parameters
    - Update firmware on the local HBA
    - Enable Boot code
    - Update EFIBoot (64-bit only)

Starting HBAnyware from the Desktop

After the HBAnyware server has been installed, access the utility from the desktop **Start** menu.

To start HBAnyware for Windows:

1. On the Windows desktop, click **Start**, **Programs /HBAnyware**.
2. Initially discovery information for the host appears:

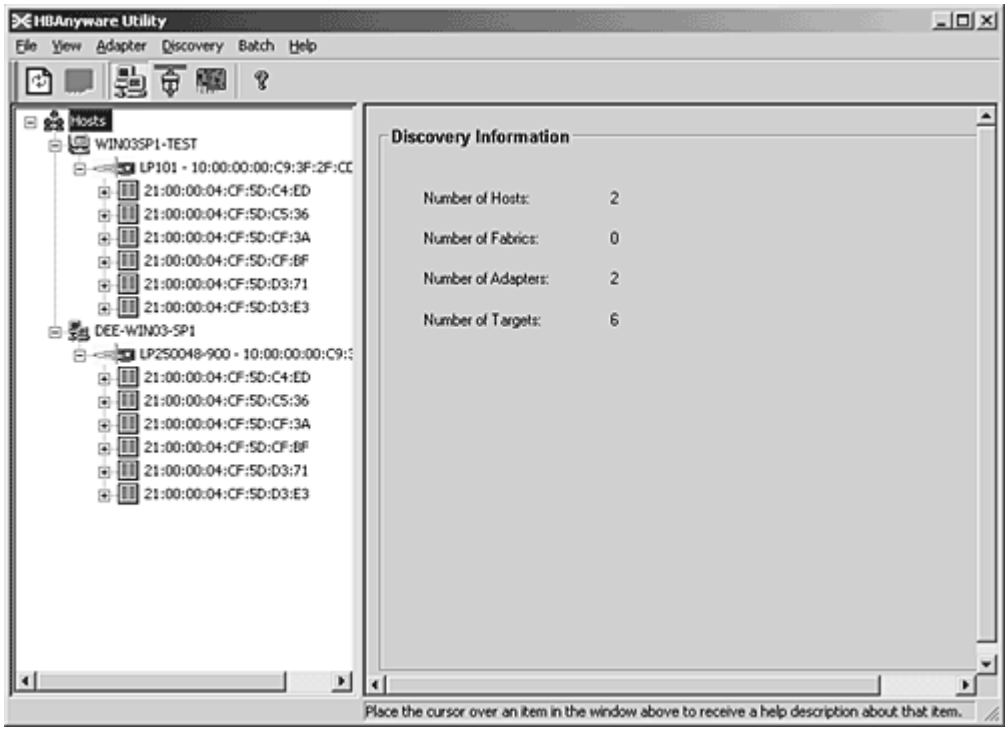

Figure 6: HBAnyware Utility, Discovery Information (Example)

The HBAnyware utility contains five basic elements: the menu bar, the toolbar, the discovery-tree, the property tabs and the status bar.

Note: The element that you select in the discovery-tree determines whether a menu item or toolbar icon is active. For example, if you select the local host or other system host, the **Reset Adapter** item on the **Adapter** menu becomes unavailable. The **Reset Adapter** toolbar button becomes unavailable as well.

Changing Management Mode

During installation you selected a management mode, however you can change it if the **“Allow users to change management mode from the utility"** box was checked.

HBAnyware enables you to choose three types of host/HBA management:

- Strictly Local Management - This setting only allows management of HBAs on this host. Management of HBAs on this host from other hosts is not allowed.
- Local Management Plus - This setting only allows management of HBAs on this host, but management of HBAs on this host from another host is possible.
- Full Management - This setting enables you to manage HBAs on this host and other hosts that allow it.

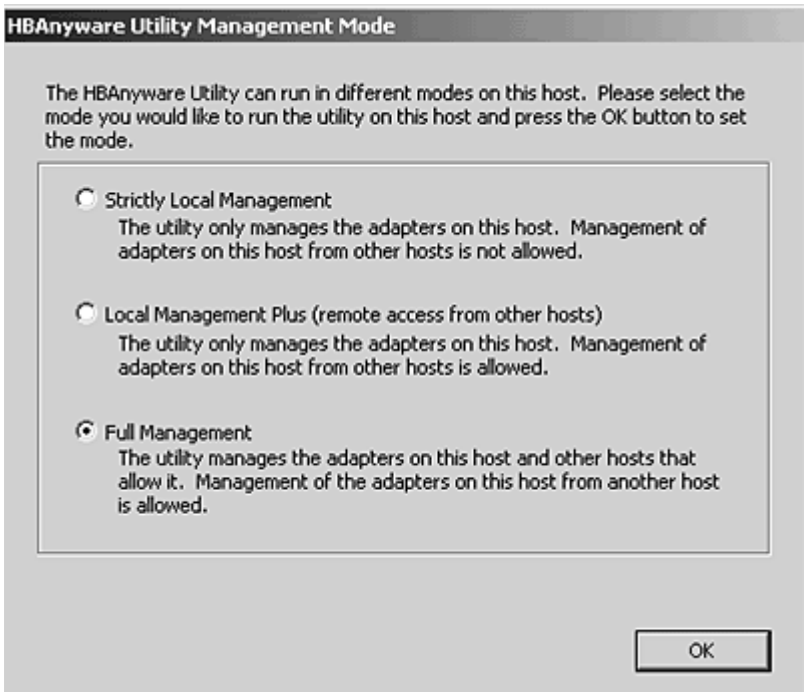
HBAnyware Utility Management Mode
The HBAnyware Utility can run in different modes on this host. Please select the mode you would like to run the utility on this host and press the OK button to set the mode.
Strictly Local Management
The utility only manages the adapters on this host. Management of adapters on this host from other hosts is not allowed.
Local Management Plus (remote access from other hosts)
The utility only manages the adapters on this host. Management of adapters on this host from other hosts is allowed.
Full Management
The utility manages the adapters on this host and other hosts that allow it. Management of the adapters on this host from another host is allowed.
OK

Figure 7: HBAnyware Utility, Management Mode Window

Starting the HBAnyware Security Configurator

Note: Before you start the Security Configurator, you **must** make sure that all of the systems that are part of, or will be part of, the security configuration are online on the FC network so that they receive updates or changes made to the security configuration.

Any system already part of the security installation might not run with the proper security attributes if updates to the security configuration are made while it is offline. Any system that is part of the security installation and that is offline when the Security Configurator starts will not be available for security configuration changes even if it is brought online while the Security Configurator is running.

To start the HBAnyware Security Configurator for Windows Server 2003 or Windows 2000 Server:

1. On the desktop, click **Start**, then select **Programs/ HBAnyware Security Configurator**. The **HBAnyware Security Configurator Discovery** window appears:

Figure 8: HBAnyware Security Configurator Discovery Window

2. After discovery is completed, the HBAnyware Security Configurator appears.

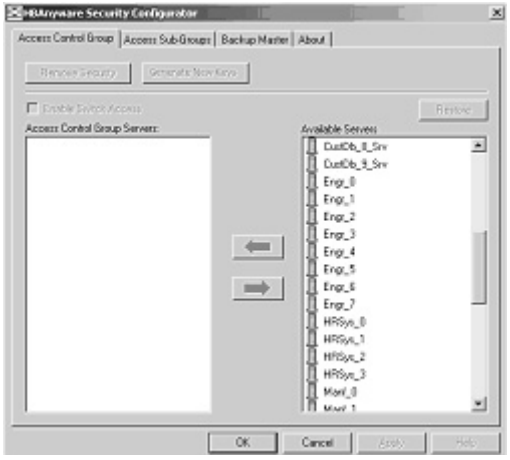

Figure 9: HBAnyware Security Configurator, Access Control Group Tab

Starting HBAnyware from the Command Line

You can launch HBAnyware from the command line. For more information on the command-line interface, see “Using the HBAnyware Command-Line Interface” on page 30.

To launch HBAnyware from the command line:

1. Type "HBAnyware" and press <ENTER>. This starts HBAnyware in in-band access. You can also start the utility in out-of-band access by adding an argument in the form "h=<host>". The <host> argument may be either the internet protocol (IP) address of the host or its system name. The call will use a default IP port of 23333, but you can override this by optionally appending a colon (:) and the IP port.

Note: Remember that not all HBAs for a specific host can run in-band. Therefore, if you run out-of-band, that host may display HBAs that do not appear when running in-band.

Note: HBAnyware can only discover and manage remote HBAs on hosts running HBAnyware's elxhbamgr. For in-band management, remote capabilities of HBAnyware are subject to fabric zoning configuration. Remote hosts you want to discover and manage by HBAnyware must be in the same zone.

Examples of Modifications

```
HBAnyware h=138.239.82.2
```

HBAnyware will show HBAs in the host with the IP address 138.239.82.2.

```
HBAnyware h=Util01
```

HBAnyware will show HBAs in the host named Util01.

```
HBAnyware h=138.239.82.2:4295
```

HBAnyware will show HBAs in the host with the IP address 138.239.82.2 using IP Port 4295.

```
HBAnyware h=Util01:4295
```

HBAnyware will show HBAs in the host named Util01 using IP port 4295.

Run this modified command line to launch HBAnyware for a single, remote host in local mode.

HBAnyware Window Element Definitions

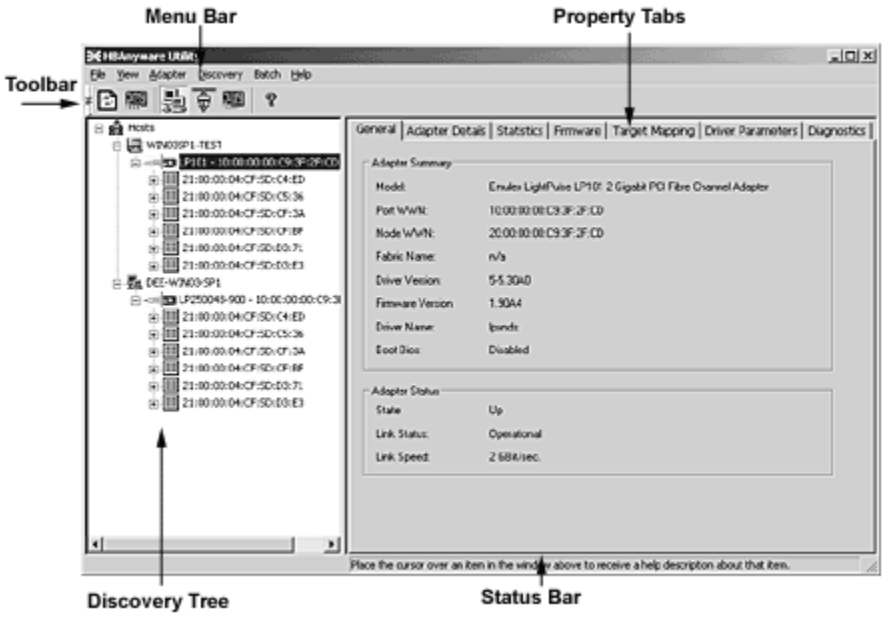

Figure 10: HBAnyware Utility Window with Element Call Outs

The Menu Bar

The menu bar contains command menus that enable you to perform a variety of tasks such as exiting HBAnyware, resetting HBAs and sorting items in the discovery-tree. Many of the menu bar commands are also available from the toolbar.

The Toolbar

The toolbar contains buttons that enable you to refresh the discovery-tree, reset the selected HBA and sort the discovery-tree. The toolbar is visible by default. Many of the toolbar functions are also available from the menu bar.

Use the Toolbar item in the View menu to hide/view the toolbar. If the menu item is checked, the toolbar is visible.

The Toolbar Buttons

Click the **Rediscover** button to refresh the discovery-tree display.

Click the **Reset** button to reset the selected HBA.

Sort Toolbar Buttons

Sort discovered HBAs by host name, fabric addresses or local HBAs. By default, HBAs are sorted by host name, with local HBAs appearing first.

Show only local or remote HBAs. See page 52 for details on sorting icons.

Sort by host name (default)

Sort by fabric address

Local HBAs only

Help

Discovery-Tree

The discovery-tree (left pane) shows icons that represent discovered network storage area network (SAN) elements (local host name, system host names and all HBAs active on each host). Targets and LUNs, when present, are also displayed.

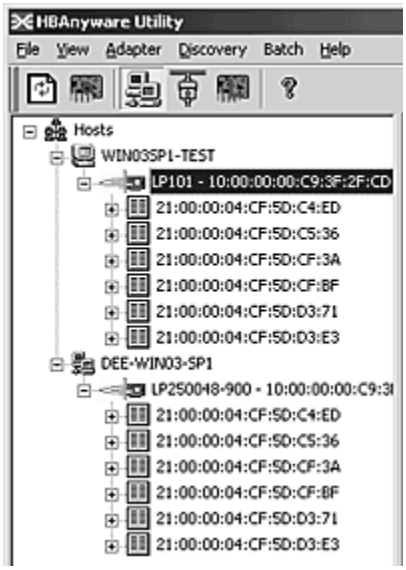

Figure 11: ***HBAnyware Utility, Discovery-Tree***

Discovery-Tree Icons

Discovery-tree icons represent the following:

The local host.

Other hosts connected to the system.

A green HBA icon with black descriptive text represents an online HBA.

A gray HBA icon with red descriptive text represents an HBA that is offline or otherwise temporarily inaccessible. Several situations could cause an offline or inaccessible HBA:

- The HBA on a local host is not connected to the network but is still available for local access.
- The HBA on a local host has malfunctioned and is inaccessible to the local host as well as the network.
- The HBA on a local host is busy performing a local download and therefore temporarily inaccessible to the local host as well as the network.

The Target icon represents connections to individual storage devices.

The LUN icon represents connections to individual LUNs.

Property Tabs

The property tabs display configuration, statistical and status information for network elements. The set of available tabs is context-sensitive, depending on the type of network element or HBA currently selected in the discovery-tree.

Status Bar

As you navigate through the menu bar or the toolbar, help messages appear on the status bar near the bottom of the HBAnyware window.

The status bar is visible by default. Use the Status Bar item in the View menu to hide the status bar. If checked, the status bar is visible.

Using the HBAnyware Command-Line Interface

The CLI (command-line interface) Client component of HBAnyware provides access to the capabilities of the Remote Management library from a console command prompt. Use this component in scripted operations from within shell scripts, batch files, or the specific platform equivalent.

Note: HBAnyware can only discover and manage remote HBAs on hosts running HBAnyware's elxhbamgr.

For in-band management, remote capabilities of HBAnyware are subject to fabric zoning configuration. Remote hosts you want to discover and manage by HBAnyware must be in the same zone.

HbaCmd can be run in out-of-band mode if you make the first argument 'h=<host>'. For example:

```
c:\>hbacmd h=cp-hp5670 listhbas
c:\>hbacmd h=138.239.91.121 listhbas
```

The CLI Client

The CLI Client is a console application named HBACMD.EXE. Each time you run this application from the command line, a single operation is performed.

The first parameter of this command is the requested operation. When the specified operation completes, the command prompt is displayed. Most operations retrieve information about an entity on the SAN and show that information on the console.

Most of the CLI Client commands require one or more additional parameters that specify the nature of the command. A parameter used by many HBACMD commands specifies the World Wide Port Name (WWPN) of the HBA target of the command. For example, the following command displays the port attributes for the HBA with the specified WWPN:

```
c:\>hbacmd portattrib 10:00:00:00:c9:20:20:20
```

Syntax Rules

The syntax rules for HBACMD are as follows:

- All CLI Client commands and their arguments are case insensitive.
- The requested operation must contain at least three characters, or as many as needed to distinguish it from any other operation.
- Whenever a WWPN is specified, individual fields are separated by colons (:) or spaces ( ). When using space separators, the entire WWPN must be enclosed in quotes (").

Out-of-Band Access

Out-of-band (OOB) access enables you to access HBAs by their IP-address or by the name of the host on which they reside. Since HBAs may exist on a host but not be a part of a Fibre Channel network, they will not appear during normal in-band discovery. Thus, OOB access enlarges the number of HBAs that you can query or modify.

Note: A local host cannot be accessed out-of-band.

OOB access via HBACMD uses an additional parameter on the command line. The parameter must be the first parameter in the list, coming immediately after HBACMD. The remaining parameters are those documented for each operation.

Note: You can also access an in-band HBA by its OOB address.

The format of the OOB parameter is:

```
h={<IPAddress> | <host-name>}
```

Some examples are:

```
h=128.239.91.88
h=cp-compaq8000
```

The following lists all HBAs running on the host with a specified IP address:

```
hbacmd h=128.239.91.88 listHBAs
```

If you don’t know the IP address, but you know the host name, enter:

```
hbacmd h=cp-compaq8000 listHBAs
```

If the host is unreachable, the command will return an error.

The CLI Client Command Reference

Version

Syntax: HBACMD Version

Description: Shows the current version of the HBAnyware CLI Client application. To view the current version, type:

```
hbacmd version
```

Sample response:

```
HBAnyware Command Line Interface: Version 3.0
```

Parameters: None.

ListHBAs

Syntax: HBACMD ListHBAs

Description: Shows a list of the discovered manageable Emulex HBAs and some of their attributes. The list will contain one 6-attribute group for each discovered HBA. Example of an attribute group list:

```
Manageable HBA List
Port WWN:   10:00:00:00:c9:20:08:cc
Node WWN:   20:00:00:00:c9:20:08:cc
Fabric Name:10:00:00:60:69:90:0b:f6
Flags:      0000f900Host Name:  CP-EMULEX-DECPC
Mfg:        Emulex Corporation
```

Parameters: None.

SaveConfig

Syntax: HBACMD SaveConfig <wwpn> <filename> <ctrlword>

Description: Saves the contents of the driver parameter list to a file for the specified HBA. The ASCII file lists parameter definitions delimited by a comma. Each definition is of the form:

```
<parameter-name>=<parameter-value>
```

Save either the values of the global set or those specific to the referenced HBA. The file created by this command stores itself in the Emulex Repository directory.

Example:

```
hbacmd SaveConfig elxstor-5-1.20A0.dpv 10:00:00:00:c9:2e:51:2e N
```

Sample response:

```
HBACMD_SaveConfig: Success writing driver parameters to file
C:\Program Files\HBAnyware\Emulex Repository\elxstor-5-1.20A.dpv
```

Parameters:

WWPN - the World Wide Port Name of the HBA (this HBA can be either local or remote).

filename - the file name that will contain the driver parameter list upon successful completion of this command.

ctrlword - G = save the global parameter set, N = save the local (HBA-specific) parameter set.

HBAAttrib

Syntax: HBACMD HBAAttrib <wwpn>

Description: Shows a list of all HBA attributes for the HBA with the specified WWPN. To view the attributes for the HBA, type:

```
hbacmd hbaattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
HBA Attributes for 10:00:00:00:c9:20:08:cc
Host Name       : CP-EMULEX-DECPC
Manufacturer    : Emulex Corporation
Serial Number   : 0000c92008cc
Model           : LP9000
Model Desc      : Emulex LightPulse LP9000 1 Gigabit PCI Fibre
Channel Adapter
Node WWN        : 20 00 00 00 c9 20 08 cc
Node Symname    : Emulex LP9000 FV3.92A2  DV5-5.20A0
HW Version      : 1002806D
Opt ROM Version:
FW Version      : 3.92A2
Vender Spec ID : 10DF
Number of Ports: 1
Driver Name     : lpxnds
Device ID       : F900
HBA Type        : LP9000
Operational FW : SLI-2 Overlay
SLI1 FW         : LP9K SLI-1 Overlay 3.92a2
SLI2 FW         : LP9K SLI-2 Overlay 3.92a2
IEEE Address    : 00 00 c9 20 08 cc
Boot BIOS       : Disabled
Driver Version : 5-5.20A0; HBAAPI v2.2.a, 10-19-04
Kernel Version : 1.30a5
```

Parameters:

WWPN - the World Wide Port Name of the HBA (this HBA can be either local or remote).

PortAttrib

Syntax: HBACMD PortAttrib <wwpn>

Description: Shows a list of all port attributes for the port with the specified WWPN. To view the port attributes for the HBA, type:

```
hbacmd portattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Port Attributes for 10:00:00:00:c9:20:08:cc
Node WWN             : 20 00 00 00 c9 20 08 cc
Port WWN             : 10 00 00 00 c9 20 08 cc
Port Symname         :
Port FCID            : 6A0200
Port Type            : Fabric
Port State           : Operational
Port Service Type    : 4
Port Supported FC4   : 00 00 01 00 00 00 00 01
                       00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00
```

```
                          00 00 00 00 00 00 00 00
Port Active FC4     : 00 00 01 00 00 00 00 01
                      00 00 00 00 00 00 00 00
                      00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00
Port Supported Speed: 1 GBit/sec.
Port Speed          : 1 GBit/sec.
Max Frame Size      : 2048
OS Device Name      : \\.\Scsi2:
Num Discovered Ports: 18
Fabric Name         : 10 00 00 60 69 30 1e 4f
```

Parameters:

WWPN - the World Wide Port Name of the HBA (this HBA can be either local or remote).

PortStat

Syntax: HBACMD PortStat <wwpn>

Description: Shows all port statistics for the HBA with the specified WWPN. To view port statistics for the HBA, type:

```
hbacmd portstat 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Port Statistics for 10:00:00:00:c9:20:08:cc

Exchange Count           :  1496534
Responder Exchange Count:  37505
TX Seq Count             :  1588007
RX Seq Count             :  1561255
TX Frame Count           :  1588695
RX Frame Count           :  1561892
TX Word Count            :  19821312
RX Word Count            :  66368000
TX KB Count              :  77427
RX KB Count              :  259250
LIP Count                :  1
NOS Count                :  n/a
Error Frame Count        :  0
Dumped Frame Count       :  n/a
Link Failure Count       :  0
Loss of Sync Count       :  9
Loss of Signal Count     :  0
Prim Seq Prot Err Count  :  0
Invalid TX Word Count    :  0
nvalid RX Frame CRC Cnt  :  0
Link Transition Count    :  0
Active RPI Count         :  0
Active XRI Count         :  0
Rx Port Busy Count       :  0
Rx Fabric Busy Count     :  0
Primary Sequence Timeout:  0
Elastic Buffer Overrun   :  0
Arbitration Timout       :  0
```

Parameters:

WWPN - the World Wide Port Name of the HBA (this HBA can be either local or remote).

ServerAttrib

Syntax: HBACMD ServerAttrib <WWPN>

Description: Shows a list of attributes of the server running locally to the specified HBA. To view the server attributes for the HBA, type:

```
hbacmd serverattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Server Attributes for 10:00:00:00:c9:20:08:cc

Host Name       : CP-EMULEX-DECPC
FW Resource Path: C:\Program Files\HBAnyware\Emulex Repository
DR Resource Path: C:\Program Files\HBAnyware\Emulex Repository
HBAnyware Server Version: 3.0
```

Parameters:

WWPN - the World Wide Port Name of any HBA local to the designated server (the HBA itself can be either local or remote).

TargetMapping

Syntax: HBACMD TargetMapping <wpm>

Description: Shows a list of mapped targets and the LUNs attached to each for the port with the specified WWPN. To view the target mapping for 10:00:00:00:c9:20:08:0c, type:

```
hbacmd targetmapping 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Target Mapping for 10:00:00:00:c9:20:08:cc

FCP ID: 10FEF
SCSI Bus Number:  1
SCSI Target Num:  0
Node WWN:  50:06:04:8A:CC:C8:99:00
Port WWN:  50:06:04:8A:CC:C8:99:00
OS Device Name :  \\.\Scsi2:1:0:0

FCP LUN 00:  0000 0000 0000 0000
SCSI OS Lun:  0
Vendor ID: EMC
Product ID:  SYMMETRIX
Product Version:  5669
SCSI Capacity:  4315 MB
Block Size:  512 Bytes

FCP ID: 10101
SCSI Bus Number:  1
SCSI Target Num:  1
Node WWN:  20:00:00:D0:B2:00:30:40
Port WWN:  20:00:00:D0:B2:00:30:40
OS Device Name:  \\.\Scsi2:1:1:0

FCP LUN 00   0000 0000 0000 0000
SCSI OS Lun:  0
Vendor ID:  XIOTECH
Product ID:  STORAGE
```

```
Product Version:   1.00
SCSI Capacity:  2009 MB
Block Size:  512 Bytes

FCP LUN 01:  0001 0000 0000 0000
SCSI OS Lun:  1
Vendor ID:   XIOTECH
Product ID:  STORAGE
Product Version:  1.00
SCSI Capacity:  2009 MB
Block Size:  512 Bytes
```

Parameters:

WWPN - the World Wide Port Name of the HBA (this HBA can be either local or remote).

Reset

Syntax: HBACMD Reset <wwpn>

Description: Resets the HBA with the specified WWPN. An HBA reset may require several seconds to complete, especially for remote devices. This command will return for additional input only after the reset has finished. To reset an HBA whose WWPN is 10:00:00:00:c9:e:51:2e, type:

```
hbacmd reset 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Reset HBA 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - the World Wide Port Name of the HBA (this HBA can be either local or remote).

Download

Syntax: HBACMD Download <wwpn> <filename>

Description: Loads the specified firmware image to the HBA with the specified WWPN. To load the firmware image located in hdc190a4.dwc to an HBA with WWPN 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd download 10:00:00:00:c9:2e:51:2e hdc190a4.dwc
```

Sample response for a successful download:

```
Downloading hdc190a4.dwc to hba 10:00:00:00:c9:2e:51:2e
Download Complete.
```

Parameters:

WWPN - the World Wide Port Name of the HBA that is the target of the firmware download (this HBA can be either local or remote).

FileName - the file name of the firmware image you want to load (this can be any file accessible to the CLI client application).

PersistentBinding

Syntax: HBACMD PersistentBinding <wwpn> <source>

Description: Queries the presence of any persistent binding for the specified WWPN. The <source> queries either the configured or live state of any present binding. To view the configured persistent binding for an HBA whose WWPN is 10:00:00:00:c9:20:0d:36, type:

```
hbacmd persistentbinding 10:00:00:00:c9:20:0d:36 C
```

Sample response:

```
Persistent Binding for 10:00:00:00:c9:20:0d:36

Bind Type      : WWPN
FCP ID         : 10101
SCSI Bus Number: 0
SCSI Target Num: 0
Node WWN       : 20:00:00:D0:B2:00:30:40
Port WWN       : 20:00:00:D0:B2:00:30:40
OS Device Name : \\.\Scsi:4:0

Bind Type      : WWPN
FCP ID         : 10FEF
SCSI Bus Number: 0
SCSI Target Num: 1
Node WWN       : 50:06:04:8A:CC:C8:99:00
Port WWN       : 50:06:04:8A:CC:C8:99:00OS
Device Name : \\.\Scsi:4:1If no such binding exists, only the
first line is returned.
```

Parameters:

WWPN - the World Wide Port Name of the HBA persistent bindings that you want to query (this HBA can be either local or remote).

Source - C if the configured state is being queried, L if the live state is being queried.

AllNodeInfo

Syntax: HBACMD AllNodeInfo <wwpn>

Description: Shows target node information for each target accessible from the specified HBA. To view the target node data for 10:00:00:00:c9:20:0d:36, type:

```
Hbacmd allnodeinfo 10:00:00:00:c9:20:0d:36
```

Sample response:

```
All Node Info for 10:00:00:00:c9:20:0d:36

Node Type      : UNKNOWN
FCP ID         : 10101
SCSI Bus Number: 0
SCSI Target Num: 0
Node WWN       : 20:00:00:D0:B2:00:30:40
Port WWN       : 20:00:00:D0:B2:00:30:40
OS Device Name : \\.\Scsi4:0:0

Node Type      : UNKNOWN
FCP ID         : 10FEF
SCSI Bus Number: 0
```

```
SCSI Target Num: 1
Node WWN       : 50:06:04:8A:CC:C8:99:00
Port WWN       : 50:06:04:8A:CC:C8:99:00
OS Device Name : \\.\Scsi4:0:1
```

Parameters:

WWPN - the World Wide Port Name of the HBA target node information that you want to query (this HBA can be either local or remote).

SetPersistentBinding

Syntax: HBACMD SetPersistentBinding <wwpn> <scope> <bindtype> <ID> \

<scsibus> <scsitarget>

Description: Sets a persistent binding between a Fibre Channel target and a SCSI bus and target. The binding can be to a target WWPN, target WWNN, or target D_ID.

To bind permanently, on behalf of HBA 10:00:00:00:c9:2e:51:2e, target WWPN 20:00:00:d0:b2:00:30:40 to SCSI bus 1, target 3, type:

```
hbacmd setpersistentbinding 10:00:00:00:c9:2e:51:2e P P \
                                    20:00:00:d0:b2:00:30:40 1 3
```

To bind immediately, on behalf of HBA 10:00:00:00:c9:2e:51:2e, target D_ID 10101 to SCSI bus 1, target 3, type:

```
hbacmd setpersistentbinding 10:00:00:00:c9:2e:51:2e I D \
                                    10101 1 3
```

If there are no errors, a response to the last example would be:

```
Set Persistent Binding for 10:00:00:00:c9:2e:51:2e I D \
                          10101 1 3
```

Parameters:

WWPN - the World Wide Port Name for which a persistent binding will be set (the HBA can be either local or remote).

scope - P = binding is permanent (survives across reboot), I = binding is immediate, B = binding is both permanent and immediate.

bindtype - P = enable binding by WWPN, N = enable binding by WWNN, D = enable binding by D_ID.

ID - Target WWPN if bindtype = P, Target WWNN if bindtype = N, Target D_ID if bindtype = D.

scsibus - the bus number of SCSI device.

scsitarget - the target number of SCSI device.

RemoveAllPersistentBinding

Syntax: HBACMD RemoveAllPersistentBinding <wwpn>

Description: Removes all persisting bindings associated with the referenced HBA. To remove all persistent bindings for 10:00:00:00:c9:21:5e:21, type:

```
hbacmd removeallpersistentbinding 10:00:00:00:c9:21:5e:21
```

Sample response:

```
Remove All Persistent Binding for 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - the World Wide Port Name of the HBA for which you want to remove all persistent bindings. (this HBA can be either local or remote).

RemovePersistentBinding

Syntax: HBACMD RemovePersistentBinding <wwpn> <bindtype> <ID> \

<scsibus> <scsitarget>

Description: Removes a persistent binding between a Fibre Channel target and a SCSI bus and target. The binding to be removed can be to a target WWPN, target WWNN, or target D_ID.

To remove, on behalf of HBA 10:00:00:00:c9:2e:51:2e, the binding between target WWPN=20:00:00:d0:b2:00:30:40 and SCSI bus 1, target 3, type:

```
hbacmd removepersistentbinding 10:00:00:00:c9:2e:51:2e P \
                                        20:00:00:d0:b2:00:30:40 1
```

To remove, on behalf of HBA 10:00:00:00:c9:2e:51:2e, the binding between target D_ID=10101 and SCSI bus 1, target 3, type:

```
hbacmd removepersistentbinding 10:00:00:00:c9:2e:51:2e D \
                                           10101 1 3
```

If no errors occur, a response to the last example would be:

```
Remove Persistent Binding for 10:00:00:00:c9:2e:51:2e D \
                                      10101 1 3
```

Parameters:

WWPN - the World Wide Port Name of the HBA for which you want to remove a persistent binding (the HBA can be either local or remote).

bindtype - P = enable binding by WWPN, N = enable binding by WWNN, D = enable binding by D_ID.

ID - Target WWPN if bindtype = P, Target WWNN if bindtype = N, Target D_ID if bindtype = D.

scsibus - the bus number of SCSI device.

scsitarget - the target number of SCSI device.

BindingCapabilities

Syntax: HBACMD BindingCapabilities <wwpn>

Description: Shows the binding capabilities present at the referenced HBA. To view the binding capabilities at 10:00:00:00:c9:21:5e:21, type:

```
hbacmd bindingcapabilities 10:00:00:00:c9:21:5e:21
```

Sample response:

```
Binding Capability for 10:00:00:00:c9:2e:51:2e
Can bind to D_ID
Can bind to WWPN
Can bind to WWNN
Can bind AUTOMAP
Can bind CONFIGURED
```

Parameters:

WWPN - the World Wide Port Name of the HBA binding capabilities that you want to query (this HBA can be either local or remote).

BindingSupport

Syntax: HBACMD BindingSupport <wwpn> <source>

Description: Shows the binding support available at the referenced HBA. To view the configured binding support for 10:00:00:00:c9:21:5e:21, type:

```
hbacmd bindingsupport 10:00:00:00:c9:21:5e:21 C
```

Sample response:

```
Binding Support for 10:00:00:00:c9:2e:51:2e

Can bind to WWPN
Can bind AUTOMAP
```

Parameters:

WWPN - the World Wide Port Name of the HBA binding support that you want to query (this HBA can be either local or remote).

source - C if the support is being queried, L if the live support is being queried.

SetBindingSupport

Syntax: HBACMD SetBindingSupport <wwpn> <bindflag>

Description: Sets the binding support(s) for the referenced HBA. To enable binding support for WWPN and Automap on HBA 10:00:00:00:c9:21:5e:21, type:

```
hbacmd setbindingsupport 10:00:00:00:c9:21:5e:21 P1
```

Sample response:

```
Set Binding Support for 10:00:00:00:c9:21:5e:21 P1
```

Parameters:

WWPN - the World Wide Port Name of the HBA binding that you want to set (this HBA can be either local or remote).

bindflag - 1 = enable support for Automap binding, 0 = disable support for Automap binding, P1 = enable support for WWPN binding and Automap, N1 = enable support for WWNN binding and Automap, D1 = enable support for D_ID binding and Automap, P0 = enable support for P, disable Automap, N0 = enable support for N, disable Automap D0 = enable support for D, disable Automap.

DriverParams

Syntax: HBACMD DriverParams <wwpn>

Description: Shows the name and values of each driver parameter for the selected HBA. To view the driver parameters for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd driverparams 10:00:00:00:c9:2e:51:2e
```

Sample (abbreviated) response:

```
Driver Params for 10:00:00:00:c9:2e:51:2e
```

Table 4: Sample DriverParams Response

IDX	string	Low	High	Def	Cur	Exp	Dyn
00	AbortStatus	0	ff	e	e	1	1
01	ARBTOV	1f4	4e20	5dc	5dc	1	5
02	BlinkTimeOut	1	1E	8	8	1	0
03	Class	1	2	2	2	1	1
04	CrfIntrpt	0	1	0	0	1	5
05	CrfMsCnt	0	3f	0	0	1	5
06	CrfRspCnt	0	ff	0	0	1	5
07	DebugMask	0	effffff	0	0	0	5
08	DisableAck0	0	1	0	0	1	5
09	DiscMethod	0	1	1	0	1	1
0a	DiscoveryDelay	0	7	0	0	1	1
0b	ElsRetryCount	1	ff	1	1	1	1
0c	ElsRjtCount	0	ff	2d	2d	1	1
0d	ElsTimeOut	0	1	0	0	1	1
0e	EmulexOption	0	7fffffff	d200	da00	1	0
0f	EnableDPC	0	1	0	1	1	1
10	ErrRetryMax	0	fffffffe	1	1	1	1
11	FrameSizeMSB	0	8	0	0	1	5
12	HardAddress	0	1	0	0	1	0
13	HlinkTimeOut	0	ff	1e	1e	1	1
14	InitialDelay	0	1	1	1	1	0
15	LinkSpeed	0	10	0	0	1	1
16	LinkTimeOut		1f4	3c	3c	1	1
17	LipFFrecovery	0	1	0	0	1	1
18	LogErrors	0	1	0	0	1	1
19	MapNodeName	0	1	0	0	1	0
1a	NodeTimeOut	0	ff	14	14	1	1
1b	QueueAction	0	2	0	0	1	1
1c	QueueDepth	1	ff	20	20	1	1
1d	QueueTarget	0	1	0	0	1	5
1e	QueueIncStep	0	100	2	2	1	1
1f	RegFcpType	0	1	1	1	1	1
20	ResetFF	0	1	0	0	1	1
21	ResetTPRLO	0	2	0	0	1	1
22	RetryNodePurge	0	1	1	1	1	1
23	RTTOV	a	ff	64	64	1	5

Parameters:

WWPN - the World Wide Port Name of the HBA driver parameters that you want to view (this HBA can be either local or remote).

DriverParamsGlobal

Syntax: HBACMD DriverParamsGlobal <wwpn>

Description: Shows the name and the global value of each driver parameter for the selected HBA. To view the global driver parameters for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd driverparamsglobal 10:00:00:00:c9:2e:51:2e
```

Sample (abbreviated) response:

```
Driver Params (Global) for 10:00:00:00:c9:2e:51:2e. Values in HEX.
```

Table 5: Sample DriverParamsGlobal Response

DX	string	Low	High	Def	Cur	Exp	Dyn
00	AbortStatus	0	ff	e	e	1	1
01	ARBTOV	1f4	4e20	5dc	5dc	1	5
02	BlinkTimeOut	1	1E	8	8	1	0
03	Class	1	2	2	2	1	1
04	CrfIntrpt	0	1	0	0	1	5
05	CrfMsCnt	0	3f	0	0	1	5
06	CrfRspCnt	0	ff	0	0	1	5
07	DebugMask	0	effffff	0	0	0	5
08	DisableAck0	0	1	0	0	1	5
09	DiscMethod	0	1	1	0	1	1
0a	DiscoveryDelay	0	7	0	0	1	1
0b	ElsRetryCount	1	ff	1	1	1	1
0c	ElsRjtCount	0	ff	2d	2d	1	1
0d	ElsTimeOut	0	1	0	0	1	1
0e	EmulexOption	0	7fffffff	d200	da00	1	0
0f	EnableDPC	0	1	0	1	1	1
10	ErrRetryMax	0	fffffffe	1	1	1	1
11	FrameSizeMSB	0	8	0	0	1	5
12	HardAddress	0	1	0	0	1	0
13	HlinkTimeOut	0	ff	1e	1e	1	1
14	InitialDelay	0	1	1	1	1	0
15	LinkSpeed	0	10	0	0	1	1
16	LinkTimeOut		1f4	3c	3c	1	1
17	LipFFrecovery	0	1	0	0	1	1
18	LogErrors	0	1	0	0	1	1
19	MapNodeName	0	1	0	0	1	0
1a	NodeTimeOut	0	ff	14	14	1	1
1b	QueueAction	0	2	0	0	1	1
1c	QueueDepth	1	ff	20	20	1	1
1d	QueueTarget	0	1	0	0	1	5
1e	QueueIncStep	0	100	2	2	1	1

Table 5: Sample DriverParamsGlobal Response (Continued)

1f	RegFcpType	0	1	1	1	1	1
20	ResetFF	0	1	0	0	1	1
21	ResetTPRLO	0	2	0	0	1	1
22	RetryNodePurge	0	1	1	1	1	1
23	RTTOV	a	ff	64	64	1	5

Parameters: the World Wide Port Name of the HBA driver parameters that you want to view (this HBA can be either local or remote).

SetDriverParam

Syntax: HBACMD SetDriverParam <wwpn> <ctrlword> <param> <value>

Description: Changes the value of the specified driver parameter operating the referenced HBA, and designates the scope of that change. To change the value of the LinkSpeed parameter (for example) for 10:00:00:00:c9:2e:51:2e and make it permanent, type:

```
hbacmd SetDriverParam 10:00:00:00:c9:2e:51:2e p linkspeed 2
```

Sample response:

```
Set Driver Parameter linkspeed=2(p) for 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - the World Wide Port Name of the HBA parameter that you want to modify (this HBA can be either local or remote).

ctrlword - P = make change permanent, G = make change global, B = make change both permanent and global, N = make change neither permanent nor global.

param - the name of the parameter whose value you want to modify.

Value - the new value you want to assign to the parameter.

SetBootBios

Syntax: HBACMD SetBootBios <wwpn> <ctrlword>

Description: Enables or disables the Boot BIOS on the referenced HBA. To enable the Boot BIOS for 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd setbootbios 10:00:00:00:c9:2e:51:2e E
```

Parameters:

WWPN -the World Wide Port Name of the HBA Boot BIOS that you want to enable or disable (this HBA can be either local or remote).

altword - E = enable the Boot BIOS, D = disable the Boot BIOS.

PciData

Syntax: HBACMD PciData <wwpn>

Description: Shows PCI configuration data for the HBA specified by the WWPN. To show PCI configuration data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd pcidata 10:00:00:00:c9:2e:51:2e
```

Sample response:

Table 6: Sample PciData Response

Vendor ID:	ox10DF	Device ID:	0xF900
Command:	0x011F	Status:	0x02a0
Revision ID	0x01	Prog If:	0x00
Subclass:	0x04	BaseClass:	0x0C
Cache Line Size:	0x10	Latency Timer:	0x40
Header Type:	0x00	Built In Self Test:	0x00
Base Address 0:	0xFE2fc004	Base Address 1:	0x00000000
Base Address 2:	0xFE2FD804	Base Address 3:	0x00000000
Base Address 4:	0x0000E401	Base Address 5:	0x00000000
CIS:	0x00000000	Sub Vendor ID:	0x10DF
SubSystem ID:	0xF900	ROM Base Address:	0xFE300000
Interrupt Line:	0x12	Interrupt Pin:	0x01
Minimum Grant:	0xFF	Maximum Latency:	0x00

Parameters:

WWPN - the World Wide Port Name of the HBA PCI configuration data that you want to show.

Wakeup

Syntax: HBACMD wakeup <wwpn>

Description: Shows wakeup parameter data for the HBA specified by the WWPN. To show wakeup parameter data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd wakeup 10:00:00:00:c9:2e:51:2e
```

Sample response:

Wakeup Parameters:		
Initial Load:	0x02C03992	0x00103411
Flags:	0x00000000	
Boot BIOS	0x03433290	0x00101303
SLI-1:	0x06433992	0x00103411
SLI-2:	0x07433992	0x00103411
Has Expansion ROM	0	

Parameters:

WWPN - the World Wide Port Name of the HBA wakeup parameter data that you want to show.

LoopMap

Syntax: HBACMD loopmap <wwpn>

Description: Shows the arbitrated loop map data for the HBA specified by the WWPN. To show the arbitrated loop map data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd loopmap 10:00:00:00:c9:2e:51:2e
```

Below is a sample response:

```
AL_PA:
01 Local Adapter
E8 SCSI Device
E4 SCSI Device
CA SCSI Device
```

Parameters:

WWPN - the World Wide Port Name of the HBA loopmap that you want to show.

GetBeacon

Syntax: HBACMD getbeacon <wwpn>

Description: Shows the current beacon status for the HBA specified by the WWPN. To show the current beacon status for HBA 10:00:00:00:c9:2e:51:2e, type:

For example, type:

```
hbacmd getbeacon 10:00:00:00:c9:2e:51:2e
```

Possible responses are:

```
Beacon State = On
Beacons State = Off
Unable to get Beacon state, error 1
```

Parameters:

WWPN - the World Wide Port Name of the HBA beacon status that you want to show.

SetBeacon

Syntax: HBACMD setbeacon <wwpn> <state>

Description: Sets the current beacon status for the HBA specified by the WWPN. To set the current beacon status for HBA 10:00:00:00:c9:2e:51:2e to off, type:

```
hbacmd setbeacon 10:00:00:00:c9:2e:51:2e 0
```

To set the current beacon status for HBA 10:00:00:00:c9:2e:51:2e to on, type:

```
hbacmd setbeacon 10:00:00:00:c9:2e:51:2e 1
```

Possible responses are:

```
Beacon State = On
Beacons State = Off
Unable to get Beacon state, error 1
```

Parameters:

WWPN -the World Wide Port Name of the HBA beacon status that you want to set (this HBA can be either local or remote).

State - the new state of the beacon: 0 = beacon OFF, 1= beacon ON.

PostTest

Syntax: HBACMD posttest <wwpn>

Description: Runs the POST test on the HBA specified by the WWPN. Support for remote HBA is out-of-band (Ethernet) only. To run the POST test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd h=138.239.83.87 posttest 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Running POST, polling for results.....
Power On Self Test Succeeded;time to execute = 8928 ms
```

Parameters:

WWPN - the World Wide Port Name of the HBA on which to run the POST test.

EchoTest

Syntax: HBACMD echotest <wwpn1> <wwpn2> <count> <StopOnError>

Description: Runs the echo test on the HBAs specified by WWPN2.

Note: Support for remote HBA is out-of-band (ethernet) only. The EchoTest command will fail if the target WWPN does not support the ECHO ELS command.

To run the echo test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd h=138.239.83.87 echotest 10:00:00:00:c9:2e:51:2e
10:00:00:00:c9:2e:51:45 10 1
```

Sample response:

```
Echo test: polling for results......
Echo test succeeded; time to execute = 53 ms.
```

Parameters:

WWPN1 - the World Wide Port Name of the originating HBA.

WWPN2 - the World Wide Port Name of the destination (echoing) HBA.

Count - the number of times to run the test.

StopOnError - should the test be halted on Error? 0 = no halt, 1 = halt.

Loopback

Syntax: HBACMD loopback <wwpn> <type> <count> <StopOnError>

Description: Runs the loop test on the HBA specified by the WWPN.

Note: Only external Loopback tests must be run out-of-band.

To run the loop test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd h=138.239.83.87 loopback 10:00:00:00:c9:2e:51:2e 1 10 0
```

Sample response:

```
Running Loopback:  polling for results......
Loopback Test Failed; xmit errors = 3; rcv errors = 2; time to
execute = 1015 ms.
```

Parameters:

WWPN - the World Wide Port Name of the HBA on which to run the loopback test(s).

Type - Type of loopback test where: 0 = PCI LoopBack Test, 1 = Internal LoopBack Test, 2 = External LoopBack Test.

Count - The number of times to run the test (Range = 1,...10000).

StopOnError - Should the test be halted on Error? 0 = no halt, 1 = halt.

Dump

Syntax: HBACMD dump <wwpn>

Description: Runs the dump diagnostic retrieval command on the HBA specified by the WWPN. This command is supported for local HBAs only. To run the dump diagnostic retrieval command for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd dump 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN- the World Wide Port Name of the HBA on which to you want to run the dump.

DeleteDumpFiles

Syntax: HBACMD deletedumpfiles <wwpn>

Description: Deletes all dump files associated with the HBA specified by the WWPN. To delete all dump files for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd deletedumpfiles 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
HBACMD: Dump file deletion complete.
```

Parameters:

WWPN - the World Wide Port Name of the HBA dump files that you want to delete.

Starting the LightPulse Utility (lputilnt)

To start lputilnt, do one of the following:

- Click Start, Programs, Emulex and lputilnt.
- Browse to lputilnt.exe and run this command.

lputilnt Category Summaries

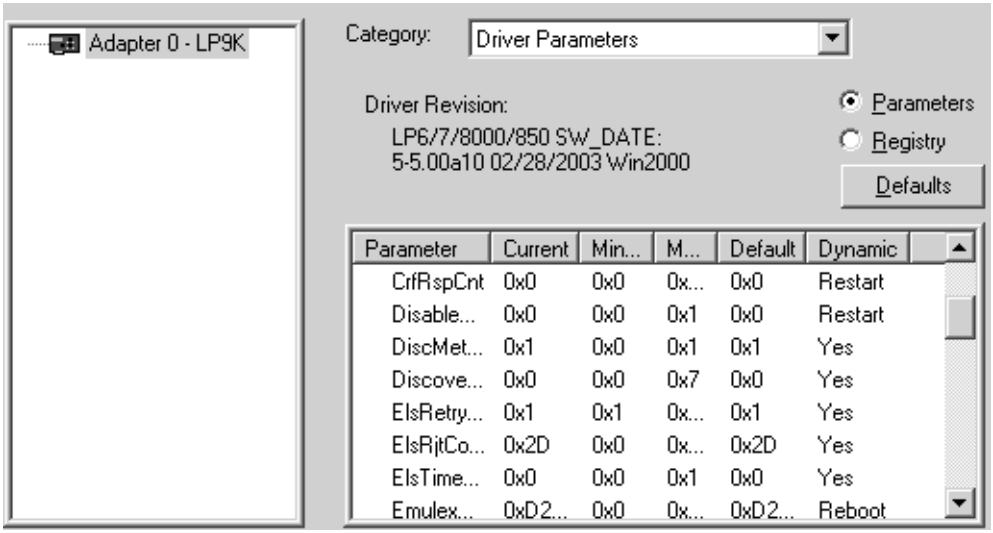

Figure 12: lputilnt Driver ParametersView

Eight categories are available:

- Adapter Revision Levels - View information about the chipset and firmware revision levels of the selected HBA.
- Firmware Maintenance - View details about the firmware in the flash read-only memory (ROM) of the selected HBA. Update HBA firmware and boot code, manage existing firmware and enable or disable the Boot bootup message.
- Loop Map - View a list of the members of the selected HBA.
- PCI Registers - View the values of the PCI configuration registers for the selected HBA.
- Configuration Data - View information about the data in each of the configuration regions in the flash ROM of the selected HBA. Download PCI configuration files (CFL).
- Driver Parameters - View and change device driver parameters.
- Persistent Binding - View and manage persistent binding for the HBA, and LUN mapping and masking for devices in your SAN.
- Link Statistics - View statistics about the arbitrated loop of the selected HBA.
- Status and Counters - View status and counters for bytes, frames, sequences, exchanges, and so on.

Discovering HBAs

- HBAnyware allows you to discover both local and remote HBAs.
- lputilnt allows you to discover local HBAs only.

Discovering HBAs with HBAnyware

Local and remote HBAs are discovered automatically when you launch HBAnyware. Initially, both local and remote HBAs appear. You can also discover HBAs on out-of-band (OOB) hosts.

Note: HBAnyware must be installed and the elxhbamgr process(es) must be running on all remote hosts that you want to discover and manage. For in-band management, remote capabilities of HBAnyware are subject to fabric zoning configuration. Remote hosts that you want to discover and manage by HBAnyware must be in the same zone.

Configuring Discovery Settings

Use the **HBAnyware Discovery Properties** dialog box to configure several discovery server parameters. You can define when to start the discovery server, when to refresh in-band and out-of-band discoveries and when to remove previously discovered HBAs that are no longer being discovered.

To configure discovery settings:

1. Start HBAnyware.

2. From the Menu bar, select Discovery/Modify Settings. The HBA Discovery Properties dialog box appears:

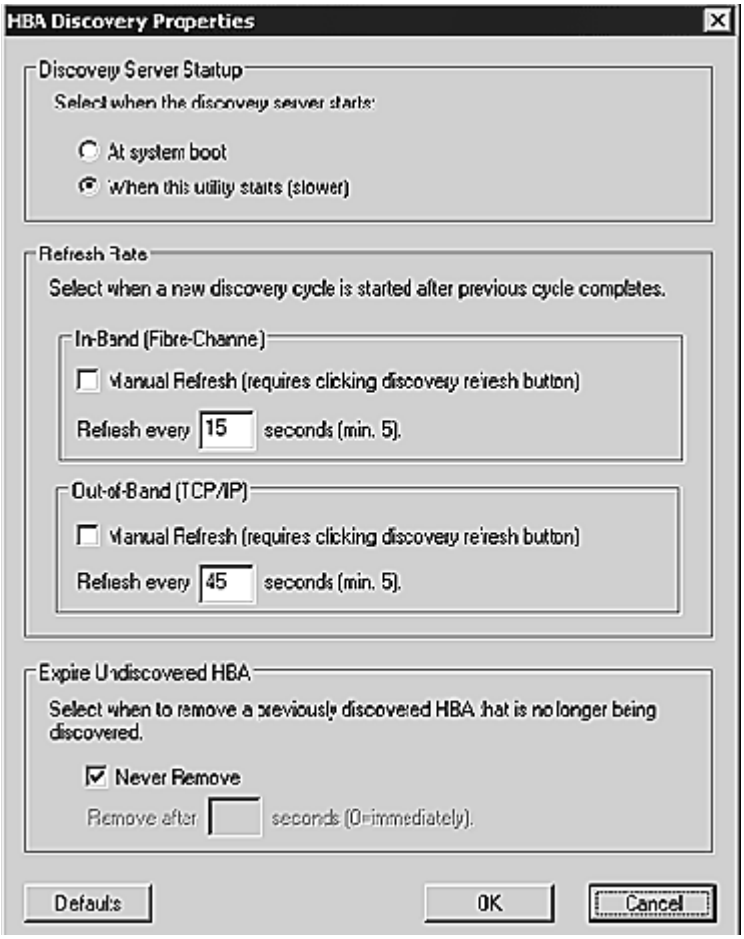
HBA Discovery Properties
Discovery Server Startup
Select when the discovery server starts:
At system boot
When this utility starts (slower)
Refresh Rate
Select when a new discovery cycle is started after previous cycle completes.
In-Band (Fibre Channel)
Manual Refresh (requires clicking discovery refresh button)
Refresh every 15 seconds (min. 5).
Out-of-Band (TCP/IP)
Manual Refresh (requires clicking discovery refresh button)
Refresh every 45 seconds (min. 5).
Expire Undiscovered HBA
Select when to remove a previously discovered HBA that is no longer being discovered.
Never Remove
Remove after seconds (0=immediately).
Defaults
OK
Cancel

Figure 13: HBAnyware Utility, HBA Discovery Properties Dialog Box

3. Define the discovery properties you wish and click **OK**. Click **Defaults** to return the discovery properties to their default settings.

Discovering HBAs Using lputilnt

Local HBAs are discovered automatically when you launch lputilnt.

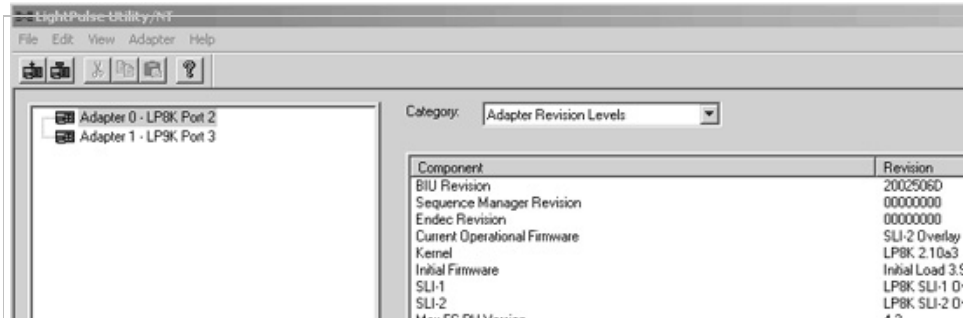

Figure 14: lputilnt Utility, HBA Information (Partial View)

Resetting the HBA

Resetting the HBA with HBAnyware

To reset the HBA:

1. Start HBAnyware.
2. In the directory-tree, click the HBA you want to reset.
3. Do one of the following:
   - From the menu bar, click **Adapter**, and then **Reset Adapter**.
   - Click the button.
4. The following warning screen appears:

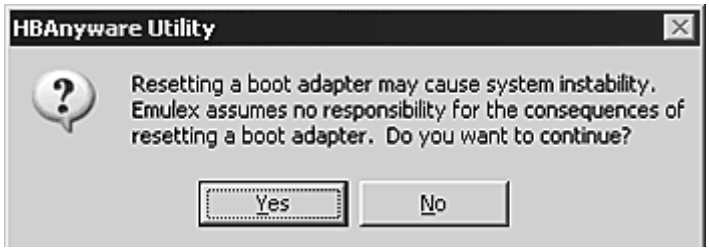
HBAnyware Utility
Resetting a boot adapter may cause system instability. Emulex assumes no responsibility for the consequences of resetting a boot adapter. Do you want to continue?
Yes
No

Figure 15: HBAnyware Utility, Reset Warning Screen

5. Click **Yes** on the warning screen to proceed with the reset.

The reset may require several seconds to complete. While the HBA resets, “Reset in progress” is displayed in the status bar. “Ready” is displayed in the status bar when reset has finished.

Resetting the HBA with lputilnt

To reset the local HBA:

1. Start lputint.
2. In the left pane, click the HBA you want to reset.
3. Do one of the following:
   - From the menu bar:

     Click **Adapter**, and then click **Reset Adapter**.
   - From the toolbar:

     Click the **Reset Adapter** button.

Resetting the HBA runs self tests and re-establishes links (causes discovery of devices). Once the HBA has been successfully reset, lputilnt is displayed.

Sorting HBA Information

Sorting HBAs with HBAnyware

Sort discovered HBAs by host name, fabric name, HBA name, target name and LUN name. You can also choose to view local HBAs or remote HBAs. By default, both local and remote HBAs are sorted by host name/fabric name.

To sort HBAs:

1. Start HBAnyware.
2. Switch between host name or fabric ID in one of two ways:
    - From the menu bar: click View, then click **Sort by Host Name** or **Sort by Fabric ID**. The current adapter display mode is checked.
    - From the toolbar, click one of the following buttons:

      Sort HBAs by Host Name (default).

      Sort HBAs by Fabric ID.
3. HBAnyware sorts in ascending order. The sort recognizes letters, numbers, spaces and punctuation marks.

Sorting by Host Name

- Initially sorts by host name. You cannot change host names using HBAnyware; names must be changed locally on that system.
- Within each host system, sorts by HBA model.
- If multiple HBAs have the same model number, sorts models by WWNN.
- If targets are present, sorts by WWPN. Multiple HBAs may refer to the same target.
- If LUNs are present, sorts by LUN name.

Sorting by Fabric Address

- Initially sorts by fabric ID.
- Within each fabric ID, sorts by HBA model.
- If multiple HBAs have the same model number, sorts models by WWNN.
- If targets are present, sorts by WWPN. Multiple HBAs may refer to the same target.
- If LUNs are present, sorts by LUN name.
- If the fabric ID is all zeros, no fabric attachment is present.

Sorting Local HBAs Only with HBAnyware

Shows HBA's local or remote location and is either on or off. Works in conjunction with the **Sort by Host Name** and **Sort by Fabric ID** buttons.

To display local HBAs only, do one of the following:

- From the menu bar: click **View**, then click **Local HBAs Only**. The current adapter display mode is checked.
- From the toolbar, click the button.

Sorting Local HBAs with lputilnt

Local HBAs are automatically displayed.

Downloading PCI Configuration Files with lputilnt

lputilnt provides information about the data in each of the configuration regions in the flash read-only memory (ROM) of the selected HBA. Select a region in the drop-down Region list, and the data contained in that region is displayed. Regions 5, 6 and 7 allow you to download PCI configuration data files to the selected region to change the PCI configuration (PCI device ID).

Note: Downloading PCI configuration files is not applicable to the following Emulex HBAs: LP982, LP952L and LP850.

Caution: Download PCI configuration files only with the assistance of Emulex technical support.

Viewing HBA Information Using HBAnyware

Viewing Discovered Information

Discovery information contains a general summary of the discovered elements. The **Host** or **Fabric** icon, depending upon which view is selected, is the root of the discovery-tree, but it does not represent a specific network element. Expanding it will reveal all hosts, LUNs, targets and HBAs that are visible on the SAN.

To view the discovery information:

1. Start HBAnyware.
2. Click the **Host** or **Fabric** icon at the root of the discovery-tree. Discovered SAN elements appear in the discovery-tree. Select an element from the discovery-tree to learn more about it.

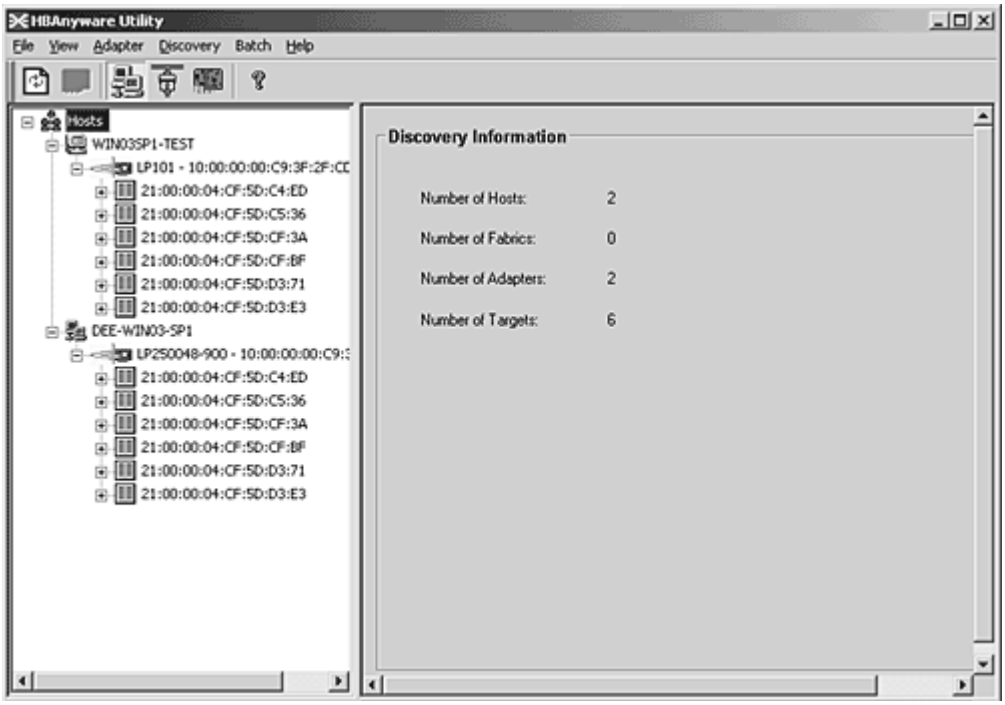

Figure 16: HBAnyware Utility, Discovery Information

Discovery Information Field Definitions

- Number of Hosts - the total number of host computers discovered. This includes servers, workstations, personal computers, multiprocessors and clustered computer complexes.
- Number of Fabrics - the total number of fabrics discovered.
- Number of Adapters - the total number of HBAs discovered.
- Number of Targets - the total number of unique targets discovered on the SAN. In the discovery-tree, the same target can appear under more than one HBA.

Viewing Host Information

There are two tabs that show host information: the Host Information tab and the host Driver Parameters tab. The Host Information tab is read-only. The host Driver Parameters tab enables you to view and define HBA driver settings for a specific host.

To view the Host Information and Driver Parameters tabs:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then **Sort by Host Name**.
   - From the toolbar, click the button.
3. Click a host name in the discovery-tree.
4. Select the Host Information tab.

The Host Information Tab

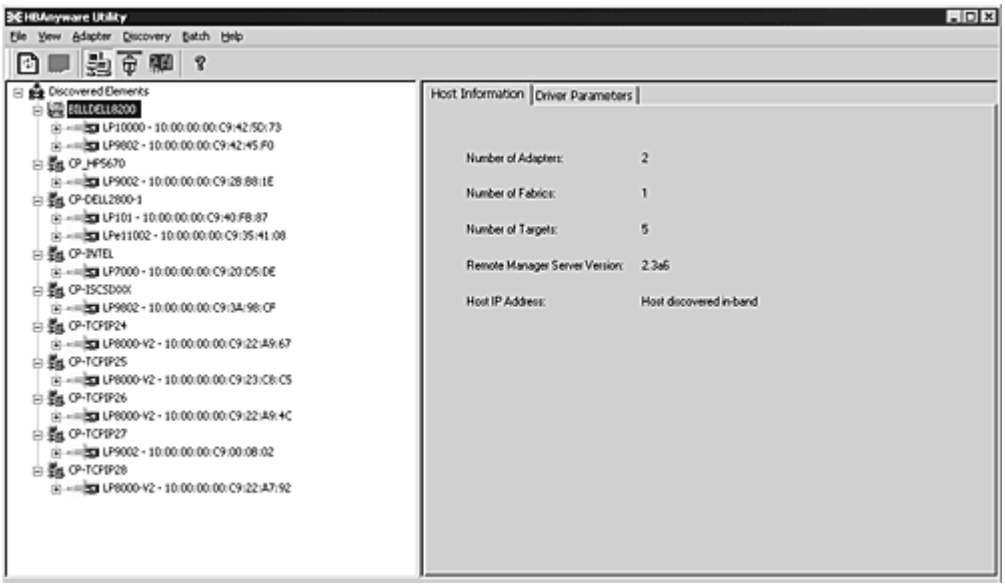

Figure 17: HBAnyware Utility, Host Information Tab

Host Information Field Definitions

- Number of Adapters - the total number of HBAs installed in the host.
- Number of Fabrics - the total number of fabrics to which the host is attached.
- Number of Targets - the number of storage devices seen by the host.

- Remote Manager Server Version - the version of the HBAnyware server running on the host. If different versions of HBAnyware are installed on different hosts in the SAN, those differences appear in this field.
- Host IP Address - if the host is discovered in-band, the dialog box displays "Host discovered in-band." If the host is discovered out-of-band, the dialog box displays the host's IP address, e.g., 138.239.82.131.

The Host Driver Parameters Tab

The host Driver Parameters tab (Figure 18) enables you to view and edit the HBA driver settings contained in a specific host. The host driver parameters are global values and apply to all HBAs in that host unless overridden by parameters assigned to a specific HBA using the HBA Driver Parameters tab. For each parameter, the tab shows the current value, the range of acceptable values, the default value, and whether the parameter is dynamic (a dynamic parameter allows the change to take effect without resetting the HBA or rebooting the system).

For more information on viewing host driver parameters, see “Viewing Driver Parameters” on page 66.

For information on changing parameters for a host, see “Setting Host Parameters Using HBAnyware” on page 69.

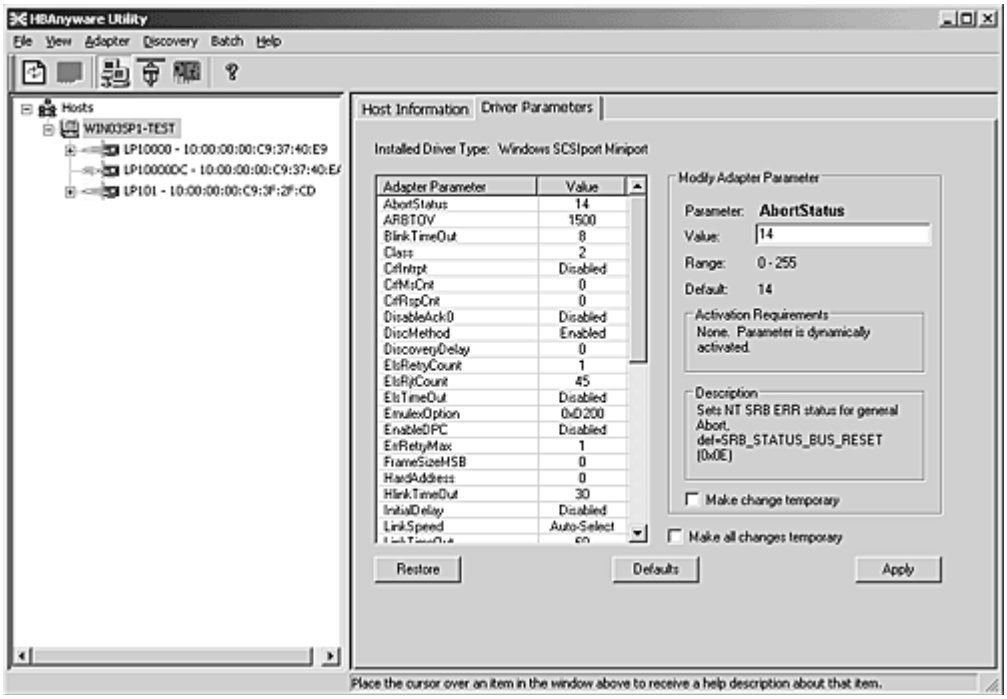

Figure 18: HBAnyware Utility, Driver Parameters Tab - Host Selected

Note: If you have more than one driver type installed, the Installed Driver Types menu shows a list of all driver types and driver versions installed on the HBAs in the host.

Viewing General HBA Information

The General tab contains general information associated with the selected HBA.

To view general attributes:

1. Start HBAnyware.
2. Select **Host** or **Fabric** sort.
3. Click an HBA in the discovery-tree.

   The General tab is displayed.

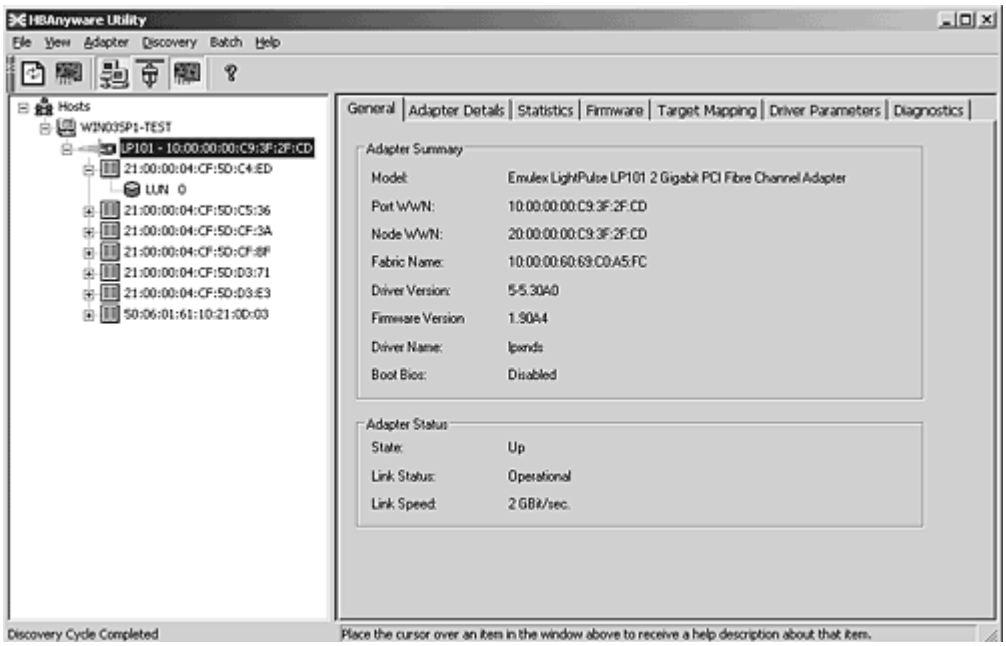

Figure 19: HBAnyware Utility, General Tab

Adapter Summary Field Definitions

Model - the Emulex HBA model number.

Port WWN - the Port World Wide Name of the HBA.

Node WWN -the Node World Wide Name of the selected HBA.

Fabric Name or Host Name - the Fabric Name field shows if you selected, “Sort by Host Name.” The fabric name is a 64-bit worldwide unique identifier assigned to the fabric. The Host Name field shows if you selected “Sort by Fabric ID.” The host name is the name of the host containing the HBA.

Driver Version - the version of the driver installed for the HBA.

Firmware Version - the version of Emulex firmware currently active on the HBA.

Driver Name - the executable file image name for the driver as it appears in the Emulex driver download package.

Boot BIOS - indicates if the boot code is enabled or disabled.

Adapter Status Field Definitions

- State - The current operation state of the HBA: “Up” or “Down”.
- Link Status - the current link status between the HBA and the fabric. There are several possible states:
  - The operational state indicates the HBA is connected to the network and operating normally.
  - All other states indicate the HBA is not connected to the network. Gray HBA icons with red descriptive text indicate an offline HBA. These offline states are:
    - User offline - the HBA is down or not connected to the network.
    - Bypassed - the HBA is in FC discovery mode.
    - Diagnostic Mode - the HBA is controlled by a diagnostic program.
    - Link Down - there is no access to the network.
    - Port Error - the HBA is in an unknown state; try resetting it.
    - Loopback - an FC-1 mode in which information passed to the FC-1 transmitter is shunted directly to the FC-1 receiver. In loopback mode, the FC interface loopback signal overrides any external signal detected by the receiver.
    - Unknown - the HBA is offline for an unknown reason.
- Link Speed - the link speed of the HBA in gigabits per second.

View Detailed HBA Information

The Adapter Details tab in HBAnyware contains detailed attributes associated with the selected HBA.

To view detailed HBA information:

1. Start HBAnyware.
2. Select **Host** or **Fabric** sort.
3. Click an HBA in the discovery-tree.
4. Click the Adapter Details tab.

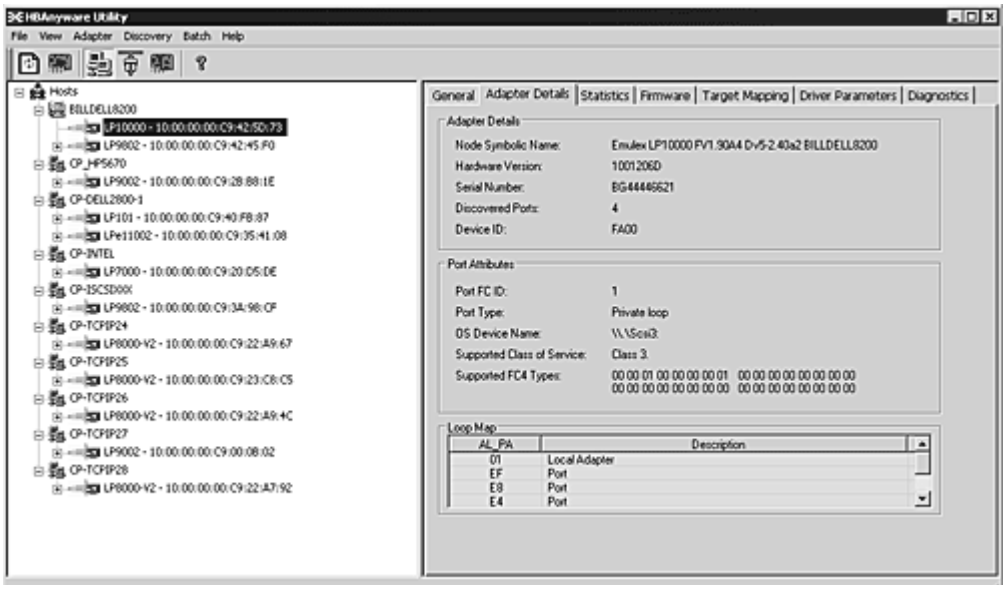

Figure 20: HBAnyware Utility, Adapter Details Tab

Adapter Details Field Definitions

- Node Symbolic Name - The Fibre Channel name used to register the driver with the name server.
- Hardware Version - the Joint Electronic Device Engineering Council identifier (JEDEC ID) of the selected HBA.
- Serial Number - the manufacturer assigned serial number of the HBA.
- Discovered Ports - the number of other HBAs visible to the selected HBA.
- Device ID - the HBA's default device ID.

Port Attributes Field Definitions

- Port FC ID - the FC ID for the port of the selected HBA.
- Port Type - the current operational mode of the selected HBA's port.
- OS Device Name - the platform-specific name by which the selected HBA is known to the operating system.
- Supported Class of Service - a frame delivery scheme exhibiting a set of delivery characteristics and attributes. There are three classes of service:
  - Class-1 provides a dedicated connection between a pair of ports with confirmed delivery or notification of nondelivery.
  - Class-2 provides a frame switched service with confirmed delivery or notification of nondelivery.
  - Class-3 provides a frame switched service similar to Class-2 but without notification of frame delivery or non-delivery.
- Supported FC4 Types - a 256-bit (8-word) map of the FC-4 protocol types supported by the port that contains the selected HBA. Each bit in the map corresponds to a type value as defined by the FC standards and contained in the Type field of the frame header.

Loop Map Table Definitions

- The loop map shows the different ports present in the loop, and is present only if the port (HBA) is operating in loop mode. The simplest example would be to connect a JBOD directly to an HBA. This port type will be a private loop, and the loop map will have an entry for the HBA, and one entry for each of the disks in the JBOD.

Viewing Fabric Attributes

Discovery Information contains information specific to the selected fabric.

To view fabric attributes:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then **Sort by Fabric ID**.
   - From the toolbar, click the button.
3. Click a fabric address in the discovery-tree. Information appears about the selected fabric.

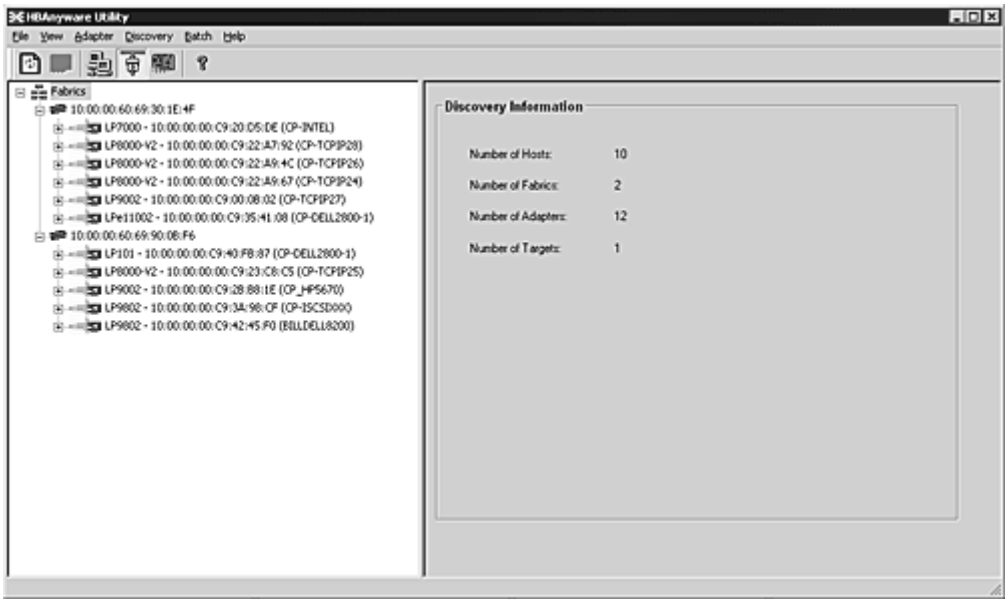

Figure 21: HBAnyware Utility, Fabric Information

Discovery Information Field Definitions

- Number of Hosts - the number of hosts discovered or seen by this host on the selected fabric.
- Number of Fabrics - the number fabrics identified during discovery.
- Number of Adapters - the number of HBAs discovered by this host on the selected fabric.
- Number of Targets - the number of storage devices seen by this host on the selected fabric.

Viewing Target Information

Target Information contains information specific to the selected storage device.

To view target information:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then click **Sort by Host Name**.
   - From the toolbar, click the button.
3. Click a target in the discovery-tree. Target Information appears.

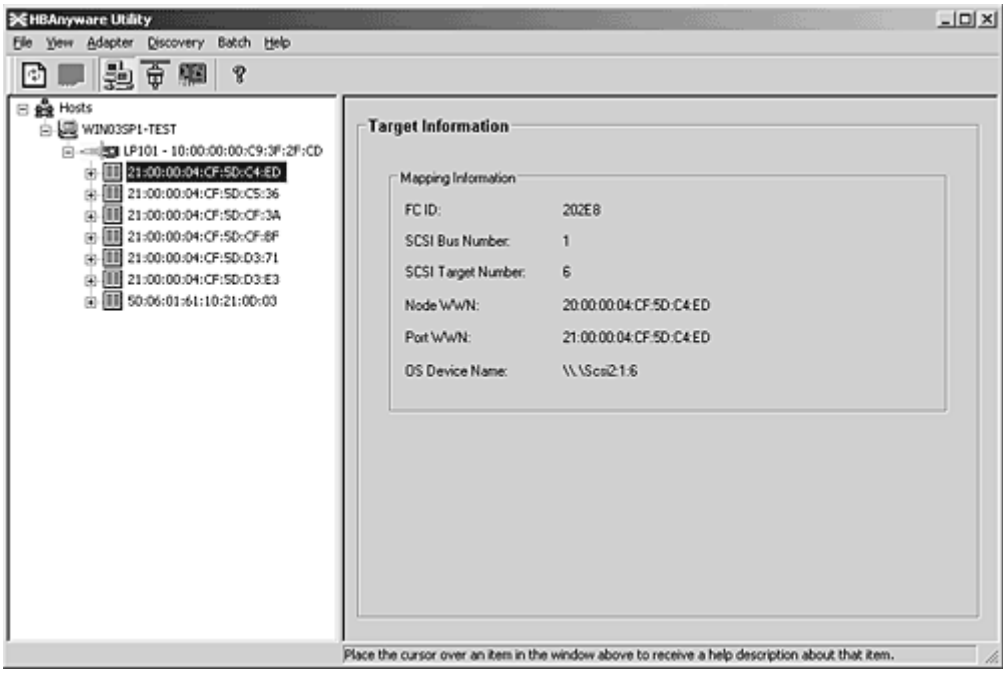

Figure 22: HBAnyware Utility, Target Information

Target Information Field Definitions

- Mapping Information
  - FC ID - the Fibre Channel (FC) ID for the target; assigned automatically in the firmware.
  - SCSI Bus Number - defines the SCSI bus to which the target is mapped.
  - SCSI Target Number - the target's identifier on the SCSI bus.
  - Node WWN - the unique 64-bit number, in hexadecimal, for the target (N_PORT or NL_PORT).
  - Port WWN - the unique 64-bit number, in hexadecimal, for the fabric (F_PORT or FL_PORT).
  - OS Device Name - the operating system device name.

Viewing LUN Information

LUN Information contains information about the selected logical unit number (LUN).

To view LUN information:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then **Sort by Host Name**.
   - From the toolbar, click the button.
3. Click a LUN in the discovery-tree.

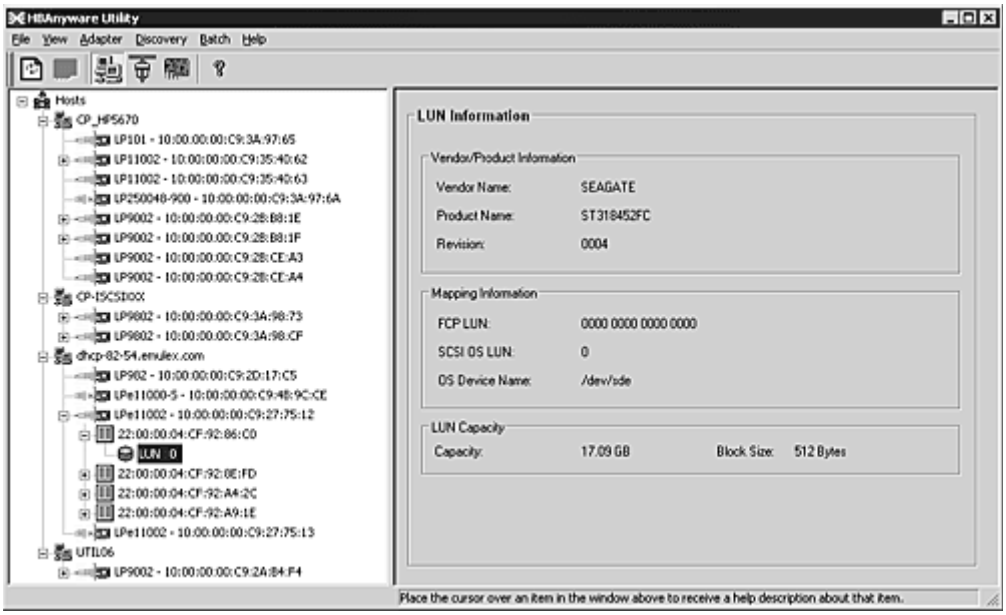

Figure 23: HBAnyware Utility, LUN Information

LUN Information Field Definitions

- Vendor Product Information Area
  - Vendor ID - the name of the vendor of the LUN.
  - Product ID - the vendor-specific ID for the LUN.
  - Revision - the vendor-specific revision number for the LUN.
- Mapping Information Area
  - FCP LUN - the FC identifier used by the HBA to map to the SCSI OS LUN.
  - SCSI OS LUN - the SCSI identifier used by the operating system to map to a specific LUN.
  - OS Device Name - the name assigned by the operating system to the selected LUN.
- LUN Capacity Area
  - Capacity - the capacity of the logical unit, in megabytes.

Note: LUN capacity information is only provided when the LUN is a mass-storage (disk) device. Other devices like tapes and scanners, etc. do not display capacity.

  - Block Size - the length of a logical unit block in bytes.

Viewing Port Statistics

The Statistics tab provides cumulative totals for various error events and statistics on the port. Statistics are cleared when the HBA is reset.

To view port statistics:

1. Start HBAnyware.
2. Select **Host** or **Fabric** sort.
3. Click an HBA in the discovery-tree.
4. Click the Statistics tab.

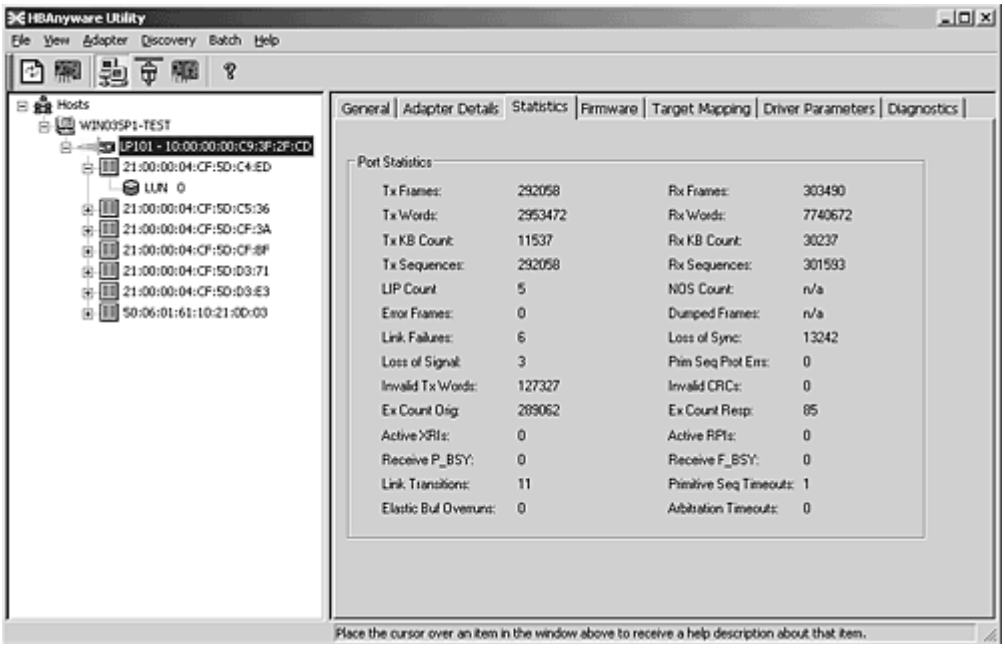

Figure 24: HBAnyware Utility, Port Statistics Tab

Port Statistics Field Definitions

- Tx Frames - FC frames transmitted by this HBA port.
- Tx Words - FC words transmitted by this HBA port.
- Tx KB Count - FC kilobytes transmitted by this HBA port.
- Tx Sequences - FC sequences transmitted by this HBA port.
- LIP count - the number of loop initialization primitive (LIP) events for the port. This field is supported only if the topology is arbitrated loop. Loop initialization consists of the following:
    - Temporarily suspend loop operations.
    - Determine whether loop capable ports are connected to the loop.
    - Assign AL_PA IDs.
    - Provide notification of configuration changes and loop failures.
    - Place loop ports in the "monitoring" state.
- Error Frames - the number of frames received with cyclic redundancy check (CRC) errors.
- Link Failures - the number of times the link failed. A link failure is a possible cause of a timeout.
- Loss of Signal - the number of times the signal was lost.

- Invalid Tx Words - the total number of invalid words transmitted by this HBA port.
- Ex Count Orig - the number of FC exchanges originating on this port.
- Active XRIs - the number of active exchange resource indicators.
- Received P_BSY - the number of FC port-busy link response frames received.
- Link Transitions - the number of times the SLI port sent a link attention condition.
- Elastic Buf Overruns - the number of times the link interface has had its elastic buffer overrun.
- Rx Frames - the number of FC frames received by this HBA port.
- Rx Words - the number of FC words received by this HBA port.
- Rx KB Count - the received kilobyte count by this HBA port.
- Rx Sequences - the number of FC sequences received by this HBA port.
- Network Operating System (NOS) count - this statistic is currently not supported for the SCSIport Miniport and Storport Miniport drivers, nor is it supported for arbitrated loop.
- Dumped Frames - this statistic is not currently supported for the SCSIport Miniport and Storport Miniport drivers.
- Loss of Sync - the number of times loss of synchronization has occurred.
- Prim Seq Prot Errs - the primitive sequence protocol error count. This counter is incremented whenever there is any type of protocol error.
- Invalid CRCs - the number of frames received that contain CRC failures.
- Ex Count Resp - the number of FC exchange responses made by this port.
- Active RPIs - the number of remote port indicators.
- Receive F_BSY - the number of FC port-busy link response frames received.
- Primitive Seq Timeouts - the number of times a primitive sequence event timed out.

Viewing Firmware Information

Use the Firmware tab to view current firmware versions and update firmware on remote and local HBAs. The update procedure is on page 102.

To view the firmware information:

1. Start HBAnyware.
2. Select **Host** or **Fabric** sort.
3. Select an HBA in the discovery-tree.
4. Select the Firmware tab.

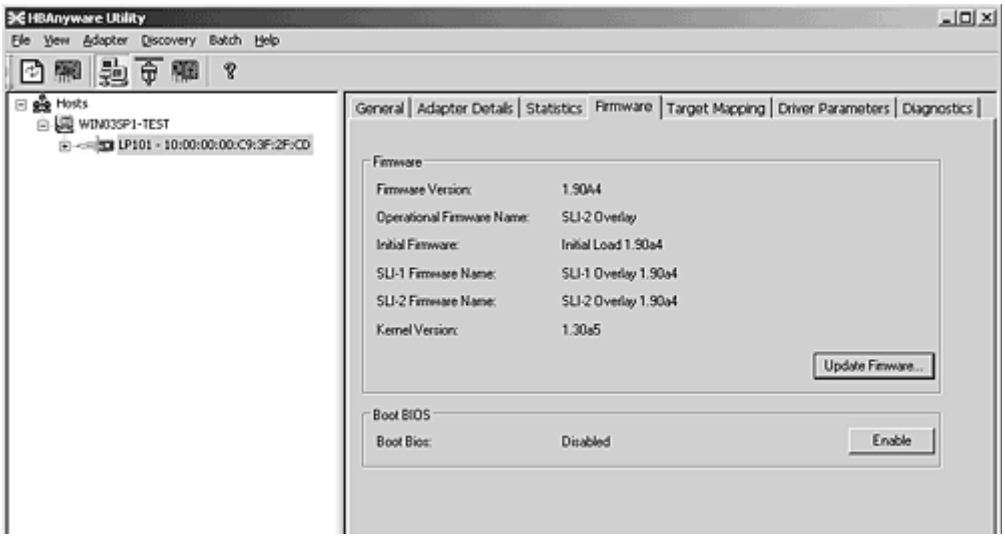

Figure 25: HBAnyware Utility, Firmware Tab (Example)

Firmware Area Field Definitions

- Firmware Version - the Emulex firmware version number for this model of HBA.
- Operational Firmware Name - if visible, the name of the operational firmware.
- Initial Firmware - the firmware version stub responsible for installing the SLI code into its proper slot.
- SLI-1 Firmware Name - the name of the SLI-1 firmware overlay.
- SLI-2 Firmware Name - the name of the SLI-2 firmware overlay.
- Kernel Version - the version of the firmware responsible for starting the driver.

Firmware Buttons

- **Update Firmware** - click to open the HBAnyware Firmware Download dialog box and update firmware. Using the HBAnyware Firmware Download dialog box, browse to the file you wish to download and download the file.
- **Enable/Disable** - click to enable or disable the boot code.

Note: If the state of the boot code has changed, this change is reflected immediately on the General tab.

Viewing Target Mapping

The Target Mapping tab enables you to view current target mapping and to set up persistent binding. Procedures begin on page 94.

To view target mapping:

1. Start HBAnyware.
2. Select **Host** or **Fabric** sort.
3. Select an HBA in the discovery-tree.
4. Select the Target Mapping tab.

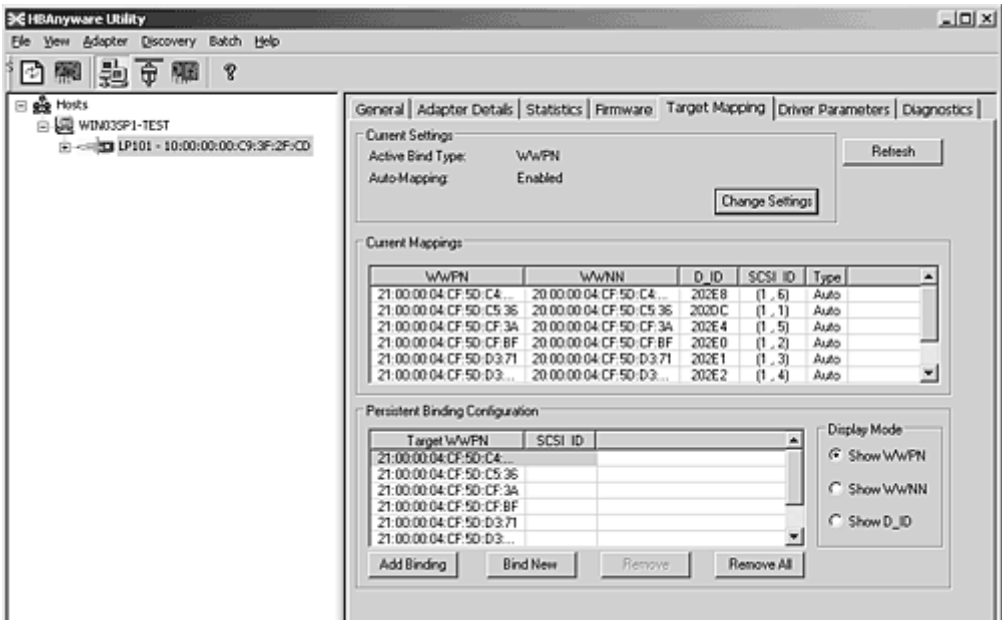

Figure 26: HBAnyware Utility, Target Mapping Tab

Target Mapping Field Definitions

Current Settings Area

- Active Bind Type - WWPN, WWNN, or a destination identifier (D_ID).
- Automapping - current state of SCSI device automapping: enabled (default) or disabled.

Current Mappings

- This table lists current mapping information for the selected HBA.

Persistent Binding Configuration

- This table lists persistent binding information for the selected HBA.

Display Mode Radio Buttons

- Show WWPN.
- Show WWNN.
- Show D_ID.

Target Mapping Buttons

- **Refresh** - click to refresh the Target Mapping tab.
- **Change Settings** - click to change the active bind type (the mode used to persistently bind target mappings), LUN automapping or LUN unmasking settings. The Mapped Target Setting window is displayed. Select the active bind type (WWPN, WWNN, D_ID or AL_PA), set LUN automapping to enabled or disabled, and/or set LUN unmasking to enabled or disabled.
- **Add Binding** - click to add a persistent binding.
- **Bind New** - click to add a target that does not appear in the Persistent Binding table.
- **Remove** - click to remove the selected binding.
- **Remove All** - click to remove all persistent bindings that are displayed.

Viewing Driver Parameters

The **Driver Parameters** tab allows you to view and modify driver parameters for all the HBAs in the host or for an individual HBA. For each parameter the tab displays the current value, the range of acceptable values, the default value, and whether the parameter is dynamic (a dynamic parameter allows the change to take effect without restarting the HBA or rebooting the system).

- For specific parameter functionality, see page 75.
- To change driver parameter values for the host, see page 69.
- To change driver parameter values for an HBA, see page 71.

Viewing Driver Parameters for an HBA

To view the driver parameters for an HBA:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then **Sort by Host Name**.
   - From the toolbar, click the button.
3. In the discovery-tree, click the HBA. The General tab is displayed.

4. Click the Driver Parameters tab (see Figure 27). The Installed Driver Types field shows the driver version installed on the HBA.

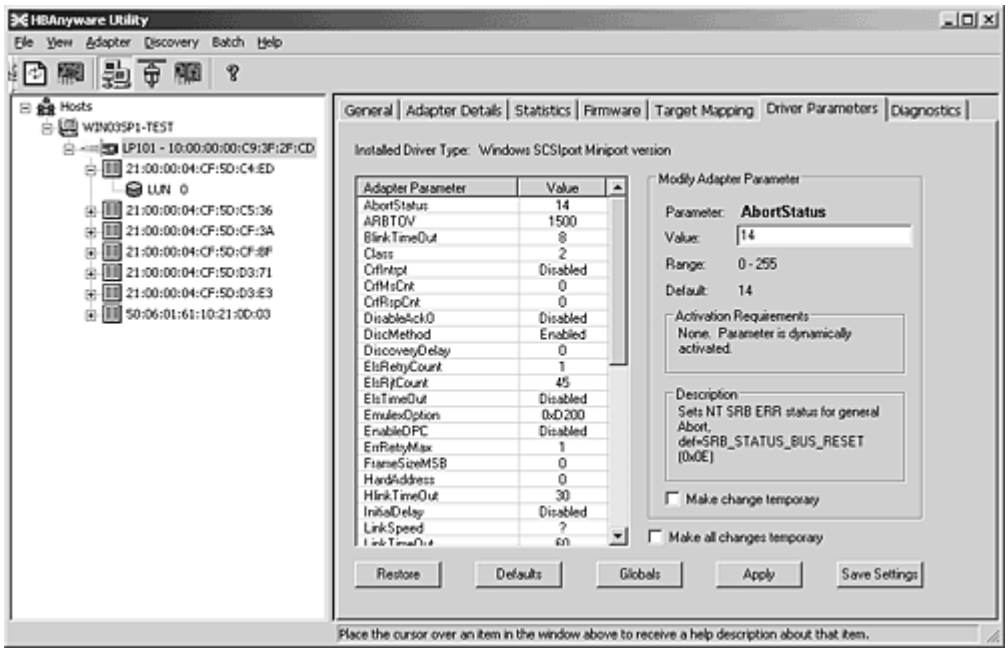

Figure 27: HBAnyware, HBA Selected, Driver Parameters Tab

Viewing Driver Parameters for All HBAs in a Host

To view the driver parameters for a host:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then **Sort by Host Name**.
   - From the toolbar, click the button.
3. In the discovery-tree, click the host. The Host Information tab is displayed.

4. Click the host Driver Parameters tab (see Figure 28). The Installed Driver Types drop-down box shows a list of all driver types and driver versions currently installed on the HBAs in the host.

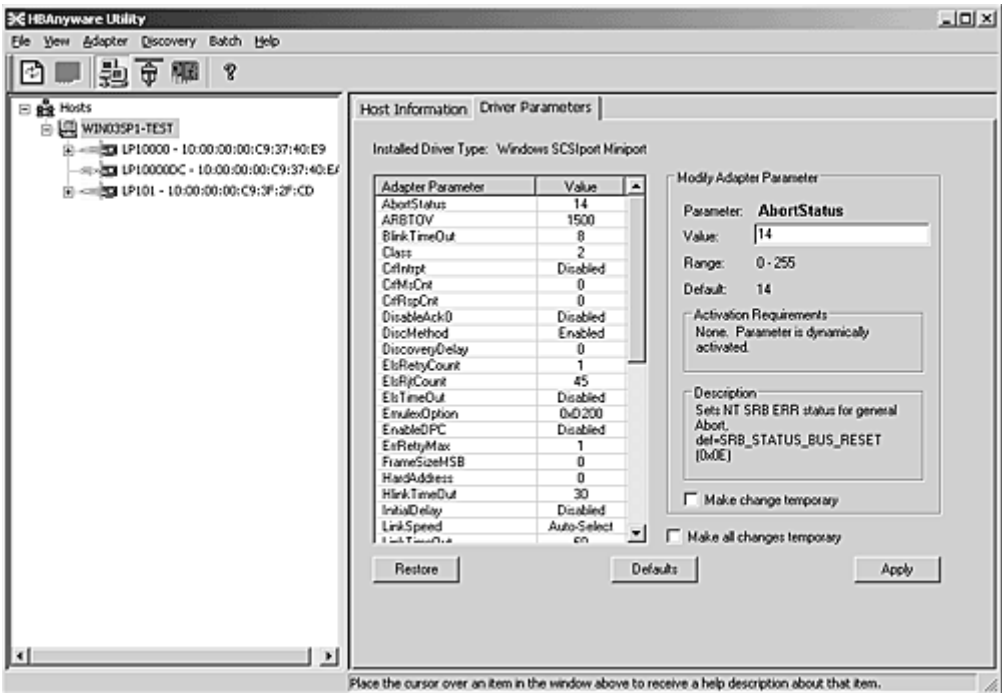

Figure 28: HBAnyware Utility, Host Driver Parameters Tab

The Driver Parameters tab and the host Driver Parameters tab have the same fields and buttons. The Driver Parameters tab corresponds to a specific HBA. The host Driver Parameter tab corresponds to all the HBAs contained in the host.

Driver Parameters Field Definitions

- Installed Driver Type - current driver and version installed.
- Adapter Parameter table - a list of parameters and their current values.
- Parameter-specific information - details about the parameter appear on the right side of the tab.

Driver Parameters Buttons

- **Restore** - click to restore parameters to this last saved value, if you have made changes to parameters and have not saved them by clicking **Apply**.
- **Defaults** - click to set all parameter values to their default (out-of-box) values.
- **Apply** - click to apply any driver parameter changes. The change may require a reboot or restart of the system.

Setting Driver Parameters

Activation Requirements

The Driver Parameters tab in HBAnyware and the Driver Parameters category in lputilnt both contain information for each parameter, including current, minimum, maximum, default settings and activation requirements.

A parameter has one of the following activation requirements:

- Dynamic - the change takes effect while the system is running.
- Reset (HBAnyware)/Restart (lputilnt) - requires an HBA reset from the utility before the change takes effect.
- Reboot - requires reboot of the entire machine before the change effect. In this case, you are prompted to do reboot when you exit the utility.

The Driver Parameter table on page 75 provides information such as the allowable range of values and factory defaults. Parameters can be entered in decimal or hexadecimal format.

Note: If you are creating custom unattended installation scripts, any driver parameter can be modified and included in the script.

Setting Host Parameters Using HBAnyware

At the host level you can specify values for specific parameters for all HBAs contained in the host. You can also set all parameters back to the default value (out-of-box value).

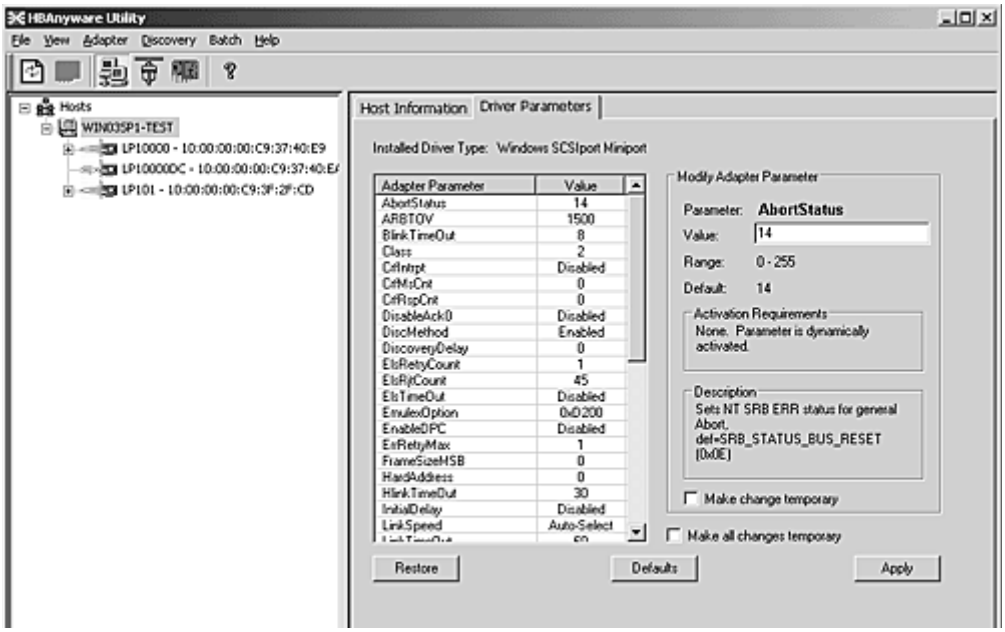

Figure 29: HBAnyware, Host Driver Parameters Tab (Example)

Setting Driver Parameters for a Host

To change the driver parameters for HBAs installed in a host:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then **Sort by Host Name**.
   - From the toolbar, click the button.
3. In the discovery-tree, select the host whose HBA driver parameters you wish to change.
4. Click the host Driver Parameters tab (Figure 29). If there are HBAs with different driver types installed, the Installed Driver Types menu shows a list of all driver types and driver version installed on the HBAs in the host. Select the driver whose parameters you wish to change. The menu does not appear if all the HBAs use the same driver.
5. In the host Driver Parameters tab, click the parameter that you want to change. A description about the parameter appears on the right side of the tab.
6. Enter a new value in the Value field. You must enter values in decimal or hexadecimal format, depending on how the current value is presented. If the value is in hexadecimal format, it is prefaced by “0x” (for example 0x2d).
7. If you want a temporary change (where the parameter reverts to its last permanent setting when the system reboots), check the "Make change temporary" box. This option is available only for dynamic parameters.
8. If you need to make changes to multiple parameters, and you want all the changes temporary, check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be made temporary.
9. Click **Apply**.

Restoring All Parameters to their Earlier Values

If you changed parameters, but did not click **Apply** and you want to restore the parameters to their last saved values, click **Restore**.

Resetting Host Parameters

To reset all host driver parameters back to their default (out-of-box) values:

1. Start HBAnyware.
2. In the discovery-tree, select the host.
3. Click the host Driver Parameters tab.
4. Click **Defaults**. Parameters to reset are displayed in red text. The following window appears:

Host Driver Parameters
You have changed some or all settings to their default values.
They will not take effect until you click Apply
OK

Figure 30: HBAnyware Utility, Host Driver Parameters Window (for defaults)

5. Click **OK** on the Host Driver Parameters window. Parameters to reset still display in red text. The value fields display the default values in red text as well.

> **Note:** If you want to set all host driver parameters back to their value before you clicked **Defaults**, click **Restore**. **Restore** will only work if you have not yet clicked **Apply**.

6. On the host Driver Parameters tab, click **Apply**.

Setting HBA Driver Parameters Using HBAnyware

To change an HBA's parameter value:

1. Start HBAnyware.
2. Do one of the following:
   - From the menu bar, click View, then **Sort by Host Name**.
   - From the toolbar, click the button.
3. In the discovery-tree, click the HBA or the host.
4. Click the Driver Parameters tab. The parameter values for the selected HBA appears.

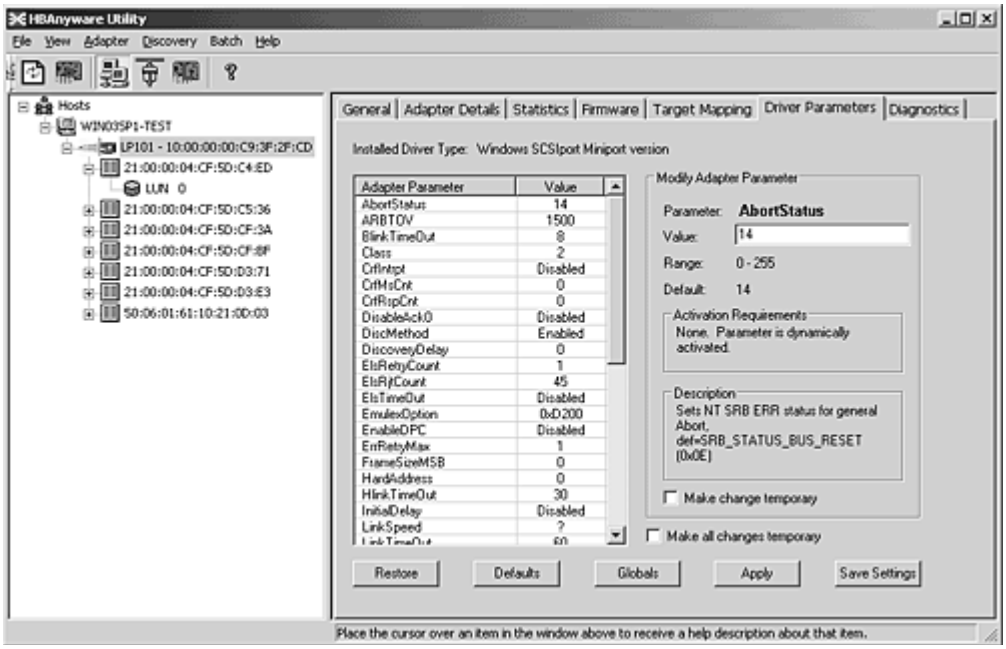

Figure 31: HBAnyware Utility, Driver Parameters Tab (Example)

5. In the Driver Parameters tab, click the parameter that you want to change. A description about the parameter appears on the right side of the tab.
6. Enter a new value in the Value field. You must enter values in decimal or hexadecimal format, depending on how the current value is presented. If the value is in hexadecimal format, it is prefaced by "0x" (for example 0x2d).
7. If you want a temporary change (where the parameter reverts to its last permanent setting when the system reboots), check the "Make change temporary" box. This option is available only for dynamic parameters.

8. If you need to make changes to multiple parameters, and you want all the changes temporary, check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be made temporary.
9. Click **Apply**.

Restoring All Parameters to Their Earlier Values

If you changed parameters, but did not click **Apply** and you want to restore the parameters to their last saved values, click **Restore**.

Resetting HBA Parameters

To reset all HBA driver parameters back to their default (out-of-box) values:

1. Start HBAnyware.
2. In the discovery-tree, select the HBA.
3. Click the Driver Parameters tab.
4. Click **Defaults**. Parameters to be reset are displayed in red text. The following window appears:

Adapter Driver Parameters
You have changed some or all settings to their default values.
They will not take effect until you click Apply.
OK

Figure 32: HBAnyware Utility, Adapter Driver Parameters Window (for defaults)

5. Click **OK** on the Adapter Driver Parameters window. Parameters to reset still display in red text. The value fields display the default values in red text as well.

> **Note:** If you want to set all the HBA's parameters back to their value before you clicked **Defaults**, click **Restore**. Restore will only work if you have not yet clicked **Apply**.

6. On the Driver Parameters tab, click **Apply**.

Saving HBA Driver Parameters to a File

To save HBA driver parameters, click **Save Settings**. Each definition is saved in a comma-delimited file with the following format:

```
<parameter-name>=<parameter-value>
```

The file is saved in the Emulex Repository directory. HBAnyware can then use the Batch Driver Parameter Update function to apply these saved settings to any or all compatible HBAs on the SAN.

Note: Persistent binding settings cannot be saved with the Save Settings feature.

Setting an HBA Parameter Value to the Host Parameter Value

To set an HBA parameter value(s) to the corresponding host parameter value(s):

1. Start HBAnyware.
2. In the discovery-tree, select the HBA.
3. Click the Driver Parameters tab.

4. Click **Globals**. All displayed values are the same as the corresponding global, or host, values. The following window appears:

Adapter Driver Parameters
You have changed some or all settings to their global values.
To take effect on this HBA, you must click Apply.
OK

Figure 33: HBAnyware Utility, Adapter Driver Parameters Window (for global values)

5. If you want a temporary change (where the parameter reverts to its last permanent setting when the system reboots), on the **D**rivers Parameters tab check the "Make change temporary" box. This option is available only for dynamic parameters.
6. If you need to make changes to multiple parameters, and you want all the changes temporary, on the Drivers Parameters tab check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be made temporary.
7. To apply your changes, click **Apply**.

Setting Parameters Using lputilnt

You can use lputilnt to change parameter values for the local HBA. You can also set all parameters back to the default value (out-of-box value) for the local HBA.

To change a driver parameter using lputilnt:

1. Start lputilnt.
2. Select an HBA.
3. Select Driver Parameters from the Category list.

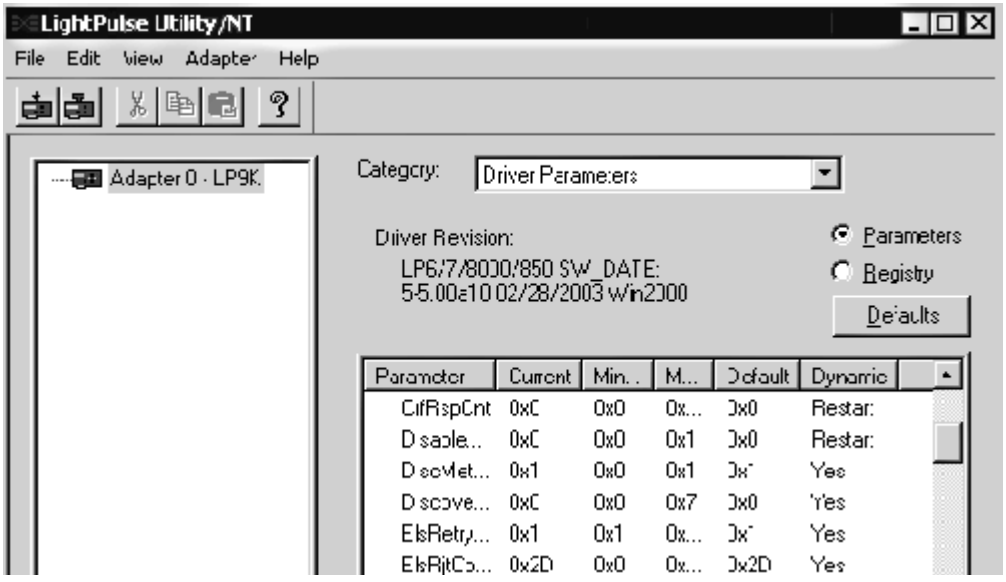

Figure 34: lputilnt Utility, Driver Parameter View

4. Double-click the parameter to edit. The Modify Driver Parameter window is displayed.

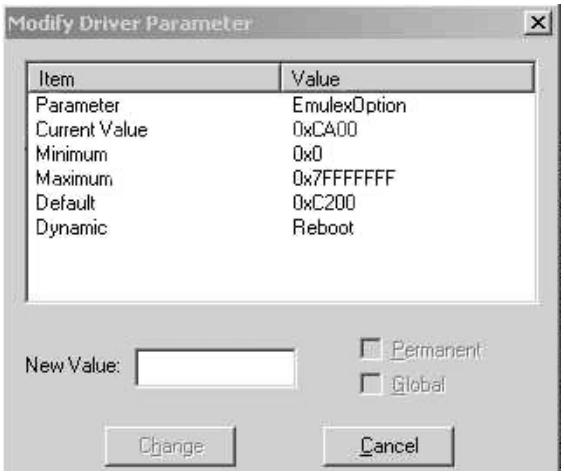

Figure 35: lputilnt Utility, Modify Driver Parameter Window

5. Enter a new value in the Value field in the same hexadecimal or decimal format as the current value. If the current value is in hexadecimal format, it is prefaced by "0x" (for example, 0x2d). You may enter a new hexadecimal value without the "0x". For example, if you enter ff10, this value is interpreted and displayed as "0xff10".
6. If desired and available, make the change permanent or global.
   - Select the Permanent box to write the new value to the system registry. If the Permanent box is not selected, the parameter reverts to its last permanent setting when the host is rebooted.
   - Select the Global box to change the global registry entry. Otherwise, the change affects the selected HBA only(Windows 2000 Server, Service Pack 3 or higher only).
7. Click **OK**.

Resetting HBA Values

To reset all the local HBA driver parameters back to their default (out-of-box) values:

1. Start lputilnt.
2. Select an HBA.
3. Select Driver Parameters from the Category list.
4. Make sure that the Parameters radio button is selected and click **Defaults**.

Figure 36: lputilnt Utility, Defaults Button

5. A confirmation window is displayed. Click **OK** on the confirmation window to set all parameters back to their defaults.

Driver Parameter Reference Table

Table 7: Driver Parameter Table

Parameter	Definition	Activation Requirement
AbortStatus = 0xn	AbortStatus controls the operating system SCSI request block (SRB) error status when the Emulex driver must return a command to the operating system for a general error condition. The default setting causes completed commands to go up to the Microsoft class driver level in Windows. Value: 0x00 to 0xFF (hex) Default = SRB_STATUS_BUS_RESET (0x0E) **Note:** Unpredictable results may occur if this value is changed.	Dynamic
ARBTOV=n	ARBTOV represents FC-AL arbitration timeout prior to LIP. Value: 500 - 20000 milliseconds Default = 1500 **Note:** Unpredictable results may occur if this value is changed.	Restart
BlinkTimeOut=n	BlinkTimeOut controls the wait time, in seconds, for the link to come up during boot. This timer only runs at boot time. Value: 1 - 30 seconds Default = 8	Reboot
Class=**n**	Class selects the class of service on FCP commands. If set to 1, class = 2. If set to 2, class = 3. Value: 1 - 2 Default = 2	Dynamic
CrfIntrpt=n	This Coalesce Response Feature must be used in conjunction with CrfMsCnt and CrfRspCnt. This feature allows the host bus adapter to hold off from interrupting the host as long as the host has made progress on the outstanding response queue during the last CrfMsCnt period. Value: 0 - 1 Default = 0	Restart
	CrfMsCnt and CrfRspCnt work together to allow better CPU utilization by processing multiple I/O responses per interrupt. Each time a response posts, the host adapter compares the current response count and, if it is greater than or equal to CoalesceRspCnt, an interrupt posts. An interrupt also posts if, after CoalesceMsCnt milliseconds, a response interrupt has not yet been posted. Zero specifies immediate response notification.	

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
CrfMsCnt=**n**	This parameter specifies wait time in milliseconds to generate an interrupt response if CoalesceRspCnt has not been satisfied. Zero specifies an immediate interrupt response notification. A non-zero value enables response coalescing at the specified interval in milliseconds. Value: 0 - 63 (decimal) or 0x0 - 0x3F (hex) Default = 0	Restart
CrfRspCnt=**n**	This parameter specifies the number of response entries that trigger an Interrupt response. Value: 0 - 255 (decimal) or 0x0 - 0xFF (hex) Default = 0	Restart
DisableAck0=n	DisableAck0 determines Class 2 ACK_0 functionality. If set to 0 = enabled. If set to 1 = disabled (ACK_1 is used). Value: 0 -1 Default = 0	Restart
DiscoveryDelay=**n**	DiscoveryDelay controls whether the driver waits for ‘n’ seconds to start port discovery after link up. If set to 0 = immediate discovery after link up. If set to 1 or 2 = the number of seconds to wait after link-up before starting port discovery. Value: 0 - 7 seconds (decimal) Default = 0 Setting this parameter >= 2 seconds helps device availability with certain target vendors. **Note**: Any target that enters PDISC pending state upon receipt of a Fabric RSCN requires this parameter to be set >=2 seconds. Check with your target vendor to determine if required.	Dynamic
DiscMethod=n	If set to 0 = issues ADISC to check existence of nodes previously logged in, before issuing PLOGI in discovery. Setting this parameter to 0 may increase compatibility to tape drives. If set to 1 = uses PLOGI only in discovery. Value: 0 -1 Default = 1	Dynamic
ElsRetryCount = n	ElsRetryCount controls how many retries to attempt when an ELS_REQUEST (such as PLOGI, PRLI, etc.) fails. Value:1 - 255 Default = 1	Dynamic

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
ElsRjtCount=n	ElsRjtCount controls how to treat LINK_SERVICE_REJECTs with either LOGICAL_BUSY/INVALID_NODE_NAME or UNABLE_PROCESS/CMO_IN_PROCESS explanations. A non-zero count allows these responses to be retried on a fixed 2-second interval for up to the value specified. Value: 0 - 255 Default = 45	Dynamic
ElsTimeOut=n	ElsTimeOut controls whether the driver reinitializes the link when two consecutive extended link service requests (such as PLOGI or PRLI) time out. If set to 1 = reinitialize link when two consecutive ELSs time out. If set to 0 = no recovery action takes place. Device discovery will continue. Value: 0 -1 Default = 0	Dynamic
EmulexOption=n	The EmulexOption hexadecimal value can be from 0x0 to 0x7FFFFFFF. n is a bit vector, one bit per option. Windows Server 2003 and Windows 2000 Server default=0x0000D200 See page 85 for more information on EmulexOption. **Note:** Changing the Emulex Option default value is not recommended unless you are running Windows 2000 Server with Service Pack 3 or above.	Reboot
EnableDPC=n	If set to 0 = process I/O completion at interrupt level. If set to 1 = process at DPC level. Value: 0 - 1 Default = 0	Dynamic
ErrRetryMax=n	ErrRetryMax specifies the number of retries while receiving an I/O error (error attention 0x10000000 [SERR or PERR]). This value may be 0 - 0xFFFFFFE. If set to 0 = retry indefinitely. If set to 1 = no retry. If set to 2 = 0xFFFFFFE : number of retries + 1. Value: 0 - 2 Default = 0x00000001	Dynamic

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
FrameSizeMSB=**n**	FrameSizeMSB controls the upper byte of receive FrameSize if issued in PLOGI. This allows the FrameSize to be constrained on 256-byte increments from 256 (1) to 2048 (8). Value: 0 - 8 Default = 0	Restart
HardAddress=n	HardAddress controls whether the driver maps addresses based on WWPN or uses the target device's D_ID. If set to 0 = map bus/target addresses to a WWPN. If set to 1 = map bus/target addresses to fixed FC-AL hard address or fabric D_ID, some hot swap applications can require HardAddress=1;. Value: 0 - 1 Default = 0	Reboot
HlinkTimeOut=0xn	HlinkTimeOut measures how long the physical link is down. HlinkTimeOut is a parameter nested inside of LinkTimeOut. HlinkTimeOut measures the timeout from hardware link-down to hardware link-up. If this timeout is exceeded, then the driver stops issuing busy status for requests and starts to issue selection_timeout error status. This value may be set smaller than LinkTimeOut as it does not include port discovery. Setting this value to 0 causes the timeout to occur after 0 seconds. Value: 0 - 255 Default = 30	Dynamic
HostName=“name”	This user-defined parameter specifies the Symbolic Node Name to register to the name server. The Symbolic Node Name needs to be surrounded by double quotation marks ("). It is limited to 32 characters in length.	Reboot
InitialDelay=n	InitialDelay controls whether the driver waits for two seconds to start port discovery at the initial link up. If set to 0 = don't wait 2 seconds at startup. If set to 1 = wait 2 seconds at startup. Value: 0 - 1 Default = 1	Reboot

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
LinkSpeed**=n**	LinkSpeed has significance only if the HBA supports speeds other than one Gbit. If set to 0 = auto link speed detection. If set to 1 = 1 Gbit. If set to 2 = 2 Gbit. If set to 4 = 4 Gbit. If set to 16 = 10 Gbit. Others = Reserved. Value: 0 - 16 (see available options) Default = 0 **Note:** Setting this option incorrectly may cause the HBA to fail to initialize.	Restart
LinkTimeOut=**n**	LinkTimeOut measures physical link down time plus how long it takes to discover remote devices. LinkTimeOut measures the timeout from when the driver no longer has “BUSYs” requests and issues selection_timeout error status. If the timer expires before discovery has completed, commands issued to timed out devices will return a SELECTION_TIMEOUT. This LinkTimeOut value includes port login and discovery time. Value: 1 - 500 seconds or 0x0 - 0xFE (hex) Default = 60 **Note:** If UseAdisc is enabled (set to 1), LinkTimeOut is enabled. If UseAdisc is disabled (set to 0), LinkTimeOut is disabled.	Dynamic
LipFFrecovery=n	LipFFrecovery controls whether the driver issues a LIP when the link has been down for LinkTimeOut/2. If set to 0 = don't issue an LIP when LinkDownTime = LinkTimeOut/2. If set to 1 = issue an LIP when LinkDownTime = LinkTimeOut/2 (helps recover some older dual-port devices). Value: 0 - 1 Default = 0	Dynamic

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
LogErrors=**n**	LogErrors allows extra event messages to log on the Windows System Event Log. Events logged by the Emulex SCSIport Miniport driver will be Event ID 11 only. Other Event IDs (i.e. 9, 15) are not logged by the Emulex SCSIport Miniport driver. You can decode Event ID 11 messages by opening up the message in Event Viewer and using the four bytes at offset 0x10 in the Event Detail. You can decode these four bytes from the tables in the online Troubleshooting manual. If set to 0 = do not log general adapter/disk errors. If set to 1 = use the event log to log general errors. Value: 0 - 1 Default = 0	Dynamic
MapNodeName=n	MapNodeName controls whether the driver maps and tracks devices based on WWPN or NodeName. If set to 0 = map devices based on WWPN. If set to 1 = map devices based on NodeName. Value: 0 - 1 Default = 0	Reboot
NodeTimeout=**n**	NodeTimeOut controls the timeout for when a formerly logged in node disappeared from the SAN. NodeTimeOut provides a delay in issuing SRB_STATUS_SELECTION_TIMEOUT errors for nodes that have disappeared from the SAN. After the timer expires, the driver makes one more attempt to re-discover the device. If that fails, the driver returns SRB_STATUS_SELECTION_TIMEOUT. The parameter value can be from 0 to 255 seconds. Setting this value to 0 causes the timeout to occur after 0 seconds. Value: 0 - 255 seconds or 0x0 - 0xFF (hex) Default = 20	Dynamic
QueueAction=n	If set to 0 = Windows Server 2003 or Windows 2000 Server QueueAction (SIMPLE_QUEUE_TAG). If set to 1 = QueueAction will be HEAD_OF_QUEUE_TAG. If set to 2 = QueueAction will be ORDERED_QUEUE_TAG. Value: 0 - 2 Default = 0 **Note:** Unpredictable results may occur if this value is changed.	Dynamic

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
QueueDepth=**n**	QueueDepth requests per LUN/target (see QueueTarget parameter). If you expect the number of outstanding I/Os per device to exceed 32, then you must increase to a value greater than the number of expected I/Os per device (up to a value of 254). If the QueueDepth value is set too low, a performance degradation can occur due to driver throttling of its device queue. Value: 1 - 255 or 0x1 - 0xFE (hex) Default = 32 (0x20)	Dynamic
QueueIncStep=n	If set to 0 = disable QueueDepth throttling down after queue full. If set to 1 - 256 = number of increment step -1 after queue full is automatically set to the number of outstanding requests -1. It begins incrementing back according to this value every second until it gets back to this original value (for example, if set to 1, the QueueDepth value does not increment back). Value: 0 -256 Default: 2	
QueueTarget=**n**	This parameter controls I/O depth limiting on a per target or per LUN basis. If set to 0 = depth limitation is applied to individual LUNs. If set to 1 = depth limitation is applied across the entire target. Value: 0 -1 or 0x0 - 0x1 (hex) Default = 0 (0x0)	Dynamic
RegFcpType=n	This parameter allows the driver to control whether the host appears as an FCP type or a general device with no type in the NameServer database. If set to 1 = register the FCP type with the name server. If set to 0 = does not register the FCP type with the name server. Value: 0 - 1 Default = 1 **Note:** Unpredictable results may occur if this value is changed.	Dynamic
ResetFF=n	ResetFFforces reservations to be freed when a ResetBus issues. This is meaningful only for FC-AL topology and Seagate native FC disk drives. If set to 0 = ResetBus action follows ResetTPRLO parameter behavior. If set to 1 = ResetBus action follows ResetTPRLO parameter behavior and completes the action with LIP (FF). Emulex recommends breaking reservations with Target Reset. Value: 0 - 1 Default = 0	Dynamic

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
ResetTPRLO=n	This parameter handles a SCSI Reset Bus call from the operating system. It is not recommended to change this value from its default or accepted OEM setting. If set to 0 = Send Target Reset Task Management commands to every logged-in target device. Send FC aborts to all outstanding commands, then re-establish a login to each target device with PLOGI and PRLI. Link reinitialization is initiated only if ResetFF=1 (not recommended). If set to 1 = Send TPRLO ELS command to every logged-in target device with Global Process Logout bit = 1 and Type Code field = 8. Link reinitialization is initiated only if ResetFF=1 (not recommended). If set to 2 = Send FC aborts to all outstanding commands, then send TPRLO to every logged-in target device with Global Process Logout bit = 1 and Type Code field = 8. Link reinitialization is initiated only if ResetFF = 1 (not recommended). Value: 0 - 2 Default = 0	Dynamic
RetryNodePurge=n	RetryNodePurge controls whether the driver causes port discovery just prior to purging a node due to NodeTimeOut exceeded. Setting this parameter to 1 allows the driver to retry discovery of a node prior to purge. This option should be enabled for all hubs that do not issue a LIP whenever a port is “un-bypassed”. The Emulex Digital hub does not require this option enabled. This parameter value can be 0 or 1. Value = 0 - 1 Default = 1	Dynamic
RTTOV=n	R_T_TOV is the receiver-transmitter timeout as specified in the ANSI FC standard. R_T_TOV represents the timeout between phases of offline to online protocol. Value = 100 - 255 milliseconds Default = 100 **Note:** Unpredictable results may occur if this value is changed.	Restart
ScanDown=**n**	If set to 0 = lowest AL_PA = lowest physical disk (ascending AL_PA order). If set to 1 = highest AL_PA = lowest physical disk (ascending SEL_ID order). Value: 0 - 1 Default = 1 **Note:** This option applies to private loop only in D_ID mode.	Reboot

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
SendEcho=n	SendEcho controls whether the driver sends an echo frame to itself every four seconds. Setting this parameter to 1 allows early detection of a spurious hub port bypass, and should be enabled for all hubs that do not issue a LIP whenever a port is 'un-bypassed'. The Emulex digital hub does not require this option enabled. Value: 0 - 1 Default = 0	Dynamic
SimulateDevice=n	If set to 0 = don't create a 'dummy' disk device. If set to 1 = create a dummy disk to force the driver to load if no disk devices present at boot time. Value: 0 - 1 Default = 0 **Note:** Microsoft provides simulate device (CreateInitiatorLU) functionality on Windows Server 2003 enabled by default during installation of the Emulex SCSIport Miniport driver, version 5.20a6. If you have a Windows Server 2003 system, use the simulate device provided by Microsoft.	Reboot
SnsALL=n	SnsAll controls which N_Ports are queried from the NameServer. If set to 0 = SCSI FCP only. If set to 1 = all N_Ports. Value: 0 - 1 Default = 0	Dynamic
TargetBlkSize=n	TargetBlkSize specifies the number of 512-byte blocks to allocate for an internal target RAM disk. This parameter is used in conjunction with the TargetEnable SCSI Target Emulator feature (see TargetEnable parameter definition). Value: 0 - 16384 Default = 16384	

Table 7: Driver Parameter Table (Continued)

Parameter	Definition	Activation Requirement
TargetEnable=n	TargetEnable allows the device driver to emulate a very simple SCSI FCP target device. To other initiators, it will appear as a small disk device of size TargetBlkSize/2 bytes. This very simple implementation only supports basic SCSI operations. Because the driver will also act as an initiator simultaneously through the same host bus adapter, the small target device will appear in the Device Manager/Disk Administrator on the host presenting the target. This parameter was designed for the test environment. If set to 0 = target disabled. If set to 1 = target enabled from boot. If set to 2 = target enabled after IOCTL. Value: 0 - 2 Default = 0 **Note:** If target mode is enabled, FCP2 is disabled.	
Topology=**n**	Topology values may be 0 to 3. If set to 0 (0x0) = FC-AL (loop). If set to 1 (0x1) = PT-PT fabric. If set to 2 (0x2) = *FC-AL first, then attempt PT-PT. If set to 3 (0x3) = *PT-PT fabric first, then attempt FC-AL. * Topology fail-over requires v3.20 firmware or higher. If firmware does not support topology fail-over, options 0,2 and 1,3 are analogous. Value: 0 - 3 Default = 2 (0x2)	Restart
TrafficCop=n	If set to 1 = enable FC-AL loop master to run unfair and break potential arbitration problems by sending frames to itself. If set to 0 = run fair, no frames all the time. Value: 0 - 1 Default = 0 **Note:** Unpredictable results may occur if this value is changed.	Restart

EmulexOption Detail

Those options with an asterisk (*) indicate that an option enabled by default.

Table 8: EmulexOption Detail

Hexadecimal Value	Description
0x00000001	DISABLE_SCSI_BUSY. DISABLE_SCSI_BUSY prevents a SCSI_BUSY error from changing the SRB status from SRB_STATUS_BUSY. errors.
0x00000002	LOG_STARTIO_ERRORS. Log all returned errors from STARTIO in the Event Log.
0x00000004	USE_BUS_RESET. This option is used only if DISABLE_SCSI_BUSY and DISABLE_SCSI_QBUSY are not set. USE_BUS_RESET allows the driver to return SRB_STATUS_BUS_RESET instead of SRB_STATUS_BUSY.
0x00000008	DISABLE_SCSI_QBUSY. DISABLE_SCSI_QBUSY prevents a SCSI_QUEUE_FULL. errors.
0x00000010	DISABLE_SCSI_RSP_CHECK. Don't validate SCSI RSP field validity.
0x00000020	Reserved.
0x00000040	Reserved.
0x00000080	LIRP_DISABLE. This option does not allow LIRP/LILP loop init phase.
0x00000100	HBA_RESET_DISABLE. Debugging option to prevent the driver from resetting the HBA.
0x00000200*	VSA_ENABLE. Allow volume set addressing.
0x00000400	Reserved.
0x00000800	Reserved.
0x00001000	Reserved.
0x00002000 0x00004000*	SERR & PERR Configuration. This is a 2-bit option. If set, bit 14 (0x00004000) will be ignored. Configure SERR & PERR as BIOS configured. If this bit is set, bit 13 (0x00002000) will be ignored. 0 for this bit turns off SERR &PERR and 1 turns on the value for SERR& PERR.
0x00008000*	SLIMPTR_ENABLE. This option enables firmware to use its memory for the host pointer instead of using host memory. This increases performance.
0x00010000	Reserved.
0x00020000	INDIV_RSTBUS. This option controls the SCSI bus reset to reset separate buses according to the pathID from the upper layer. Disable this option to allow a single bus reset to reset all SCSI buses (the standard mechanism in all previous releases).
0x00040000	FDMI_ENABLE. This option enables FDMI support.

SCSI Address Map

The driver emulates two SCSI busses and 128 targets on each bus to map 512 devices maximum. The device mapping starts on either Bus 0 or Bus 1, depending on the driver EmulexOption parameter. This table identifies the fixed mapping between Windows Server 2003 or Windows 2000 Server bus/target/LUN and the Fibre Channel native address (AL_PA/SEL_ID). There are two potential mappings based on the ScanDown parameter. Refer to the appropriate columns in the table below.
The index for the following table can be derived by:

```
#define TARGETS_PER_BUS 128
i = (Srb->PathId > 0) ? Srb->PathId-1 : 0; //Bus 0 = dummy bus
nodeInx = ((i * TARGETS_PER_BUS) + Srb-.TargetId) ;
```

* Use this translation if ScanDown = 0 (default)

** Use this translation if ScanDown = 1

** If bit 9 of EmulexOption = 0, then device addressing begins with Bus #0, not Bus #1

Table 9: SCSI Address Map

			ScanDown = 0 (default)		ScanDown = 1	
BUS #	**TARGET #**	**LUN #**	**AL_PA***	**SEL_ID***	**AL_PA****	**SEL_ID****
0	0-127	0-255	none	none	none	none
1***	0	0-255	0x01	0x7D	0xEF	0x00
	1	0-255	0x02	0x7C	0xE8	0x01
	2	0-255	0x04	0x7B	0xE4	0x02
	3	0-255	0x08	0x7A	0xE2	0x03
	4	0-255	0x0F	0x79	0xE1	0x04
	5	0-255	0x10	0x78	0xE0	0x05
	6	0-255	0x17	0x77	0xDC	0x06
	7	0-255	0x18	0x76	0XDA	0x07
	8	0-255	0x1B	0x75	0xD9	0x08
	9	0-255	0x1D	0x74	0xD6	0x09
	10	0-255	0x1E	0x73	0xD5	0x0A
	11	0-255	0x1F	0x72	0xD4	0x0B
	12	0-255	0x23	0x71	0xD3	0x0C
	13	0-255	0x25	0x70	0xD2	0x0D
	14	0-255	0x26	0x6F	0xD1	0x0E
	15	0-255	0x27	0x6E	0xCE	0x0F
	16	0-255	0x29	0x6D	0xCD	0x10
	17	0-255	0x2A	0x6C	0xCC	0x11

Table 9: SCSI Address Map (Continued)

			ScanDown = 0 (default)		ScanDown = 1	
BUS #	**TARGET #**	**LUN #**	**AL_PA***	**SEL_ID***	**AL_PA****	**SEL_ID****
	18	0-255	0x2B	0x6B	0xCB	0x12
	19	0-255	0x2C	0x6A	0xCA	0x13
	20	0-255	0x2D	0x69	0xC9	0x14
	21	0-255	0x2E	0x68	0xC7	0x15
	22	0-255	0x31	0x67	0xC6	0x16
	23	0-255	0x32	0x66	0xC5	0x17
	24	0-255	0x33	0x65	0xC3	0x18
	25	0-255	0x34	0x64	0xBC	0x19
	26	0-255	0x35	0x63	0xBA	0x1A
	27	0-255	0x36	0x62	0xB9	0x1B
	28	0-255	0x39	0x61	0xB6	0x1C
	29	0-255	0x3A	0x60	0xB5	0x1D
	30	0-255	0x3C	0x5F	0xB4	0x1E
	31	0-255	0x43	0x5E	0xB3	0x1F
	32	0-255	0x45	0x5D	0xB2	0x20
	33	0-255	0x46	0x5C	0xB1	0x21
	34	0-255	0x47	0x5B	0xAE	0x22
	35	0-255	0x49	0x5A	0xAD	0x23
	36	0-255	0x4A	0x59	0xAC	0x24
	37	0-255	0x4B	0x58	0xAB	0x25
	38	0-255	0x4C	0x57	0xAA	0x26
	39	0-255	0x4D	0x56	0xA9	0x27
	48	0-255	0x4E	0x55	0xA7	0x28
	41	0-255	0x51	0x54	0xA6	0x29
	42	0-255	0x52	0x53	0xA5	0x2A
	43	0-255	0x53	0x52	0xA3	0x2B
	44	0-255	0x54	0x51	0x9F	0x2C
	45	0-255	0x55	0x50	0x9E	0x2D
	46	0-255	0x56	0x4F	0x9D	0x2E
	47	0-255	0x59	0x4E	0x9B	0x2F
	48	0-255	0x5A	0x4D	0x98	0x30

Table 9: SCSI Address Map (Continued)

			ScanDown = 0 (default)		ScanDown = 1	
BUS #	**TARGET #**	**LUN #**	**AL_PA***	**SEL_ID***	**AL_PA****	**SEL_ID****
	49	0-255	0x5C	0x4C	0x97	0x31
	50	0-255	0x63	0x4B	0x90	0x32
	51	0-255	0x65	0x4A	0x8F	0x33
	52	0-255	0x66	0x49	0x88	0x34
	53	0-255	0x67	0x48	0x84	0x35
	54	0-255	0x69	0x47	0x82	0x36
	55	0-255	0x6A	0x46	0x81	0x37
	56	0-255	0x6B	0x45	0x810	0x38
	57	0-255	0x6C	0x44	0x7C	0x39
	58	0-255	0x6D	0x43	0x7A	0x3A
	59	0-255	0x6E	0x42	0x79	0x3B
	60	0-255	0x71	0x41	0x76	0x3C
	61	0-255	0x72	0x40	0x75	0x3D
	62	0-255	0x73	0x3F	0x74	0x3E
	63	0-255	0x74	0x3E	0x73	0x3F
	64	0-255	0x75	0x3D	0x72	0x40
	65	0-255	0x76	0x3C	0x71	0x41
	66	0-255	0x79	0x3B	0x6E	0x42
	67	0-255	0x77A	0x3A	0x6D	0x43
	68	0-255	0x7C	0x39	0x6C	0x44
	69	0-255	0x80	0x38	0x6B	0x45
	70	0-255	0x81	0x37	0x6A	0x46
	71	0-255	0x82	0x36	0x69	0x47
	72	0-255	0x84	0x35	0x67	0x48
	73	0-255	0x88	0x34	0x66	0x49
	74	0-255	0x8F	0x33	0x65	0x4A
	75	0-255	0x90	0x32	0x63	0x4B
	76	0-255	0x97	0x31	0x5C	0x4C
	77	0-255	0x98	0x30	0x5A	0x4D
	78	0-255	0x9B	0x2F	0x59	0x4E
	79	0-255	0x9D	0x2E	0x56	0x4F

Table 9: SCSI Address Map (Continued)

			ScanDown = 0 (default)		ScanDown = 1	
BUS #	**TARGET #**	**LUN #**	**AL_PA***	**SEL_ID***	**AL_PA****	**SEL_ID****
	80	0-255	0x9E	0x2D	0x55	0x50
	81	0-255	0x9F	0x2C	0x54	0x51
	82	0-255	0xAE	0x2B	0x53	0x52
	83	0-255	0xA5	0x2A	0x52	0x53
	84	0-255	0xA6	0x29	0x51	0x54
	85	0-255	0xA7	0x28	0x4E	0x55
	86	0-255	0xA9	0x27	0x4D	0x56
	87	0-255	0xAA	0x26	0x4C	0x57
	88	0-255	0xAB	0x25	0x4B	0x58
	89	0-255	0xAC	0x24	0x4A	0x59
	90	0-255	0xAD	0x23	0x49	0x5A
	91	0-255	0xED	0x22	0x47	0x5B
	92	0-255	0xB1	0x21	0x46	0x5C
	93	0-255	0xB2	0x20	0x45	0x5D
	94	0-255	0xB3	0x1F	0x43	0x5E
	95	0-255	0xB4	0x1E	0x3C	0x3C
	96	0-255	0xB5	0x1D	0x3A	0x60
	97	0-255	0xB6	0x1C	0x39	0x61
	98	0-255	0xB9	0x1B	0x36	0x62
	99	0-255	0xBA	0x1A	0x35	0x63
	100	0-255	0xBC	0x19	0x34	0x64
	101	0-255	0xC3	0x18	0x33	0x65
	102	0-255	0xC5	0x17	0x32	0x66
	103	0-255	0xC6	0x16	0x31	0x67
	104	0-255	0xC7	0x15	0x2E	0x68
	105	0-255	0xC9	0x14	0x2D	0x69
	106	0-255	0xCA	0x13	0x2C	0x6A
	107	0-255	0xCB	0x12	0x2B	0x6B
	108	0-255	0xCC	0x11	0x2A	0x6C
	109	0-255	0xCD	0x10	0x29	0x6D
	110	0-255	0xCE	0x0F	0x27	0x6E

Table 9: SCSI Address Map (Continued)

			ScanDown = 0 (default)		ScanDown = 1	
BUS #	**TARGET #**	**LUN #**	**AL_PA***	**SEL_ID***	**AL_PA****	**SEL_ID****
	111	0-255	0xD1	0x0E/	0x26	0x6F
	112	0-255	0xD2	0x0D	0x25	0x70
	113	0-255	0xD3	0x0C	0x23	0x71
	114	0-255	0xD4	0x0B	0x1F	0x72
	115	0-255	0xD5	0x0A	0x1E	0x73
	116	0-255	0xD6	0x09	0x1D	0x74
	117	0-255	0xD9	0x08	0x1B	0x75
	118	0-255	0xDA	0x07	0x18	0x76
	119	0-255	0xDC	0x06	0x17	0x77
	120	0-255	0xE0	0x05	0x10	0x78
	121	0-255	0xE1	0x04	0x0F	0x79
	122	0-255	0xE2	0x03	0x08	0x7A
	123	0-255	0xE4	0x02	0x04	0x7B
	124	0-255	0xE8	0x01	0x02	0x7C
	125	0-255	0xEF	0x00	0x01	0x7D
	126	0-255	none	none	none	none
	127	0-255	none	none	none	none

I/O Coalescing

I/O Coalescing is enabled and controlled by two driver parameters: CrfMsCnt and CrfRspCnt. The effect of I/O Coalescing will depend on the CPU resources available on the server. With I/O Coalescing turned on, interrupts are batched, reducing the number of interrupts and maximizing the number of commands processed with each interrupt. For heavily loaded systems, this will provide better throughput.

With I/O Coalescing turned off (the default), each I/O processes immediately, one CPU interrupt per I/O. For systems not heavily loaded, the default will provide better throughput. The following table shows recommendations based upon the number of I/Os per HBA

Table 10: Recommended Settings for I/O Coalescing

I/Os per Second	Suggested CrfMsCnt	Suggested CrfRspCnt	Suggested CrfIntrp
I/Os < 10000	0	8	0
10000 < I/Os < 18000	1	8	1
18000 < I/Os < 26000	1	16	1
I/Os > 26000	1	24	1

CrfMsCnt

The CrfMsCnt parameter controls the maximum elapsed time in milliseconds that the HBA waits before it generates a CPU interrupt.The value range is 0 - 63 (decimal) or 0x0 - 0x3F (hex). The default is 0 and disables I/O Coalescing.

CrfRspCnt

The CrfRspCnt parameter controls the maximum number of responses to batch before an interrupt generates. If CrfRspCnt expires, an interrupt generates for all responses collected up to that point. With CrfRspCnt set to less than 2, response coalescing is disabled and an interrupt triggers for each response. The value range for CrfRspCnt is 0 - 255 (decimal) or 0x0 - 0xFF (hex). The default value is 0.

CrfIntrpt

The CrfIntrpt parameter allows the HBA to hold off from interrupting the host as long as the host has made progress on the outstanding response queue during the last CrfMsCnt period. The default is 0 and disables the HBA's ability to hold off interrupts.

Note: A system restart is required to make changes to CrfMsCnt, CrfRspCnt and/or CrfIntrpt.

For more information on using the HBAnyware or lputilnt utilities to change driver parameter values, see "Setting Driver Parameters" on page 69.

Setting Topology

Topology Reference Table

The presence of a fabric is detected automatically.

Table 11: Topology Reference

Topology	Description	HBAnyware and lputilnt Value

Private Loop Operation	FC-AL (Loop) topology only. After successful loop initialization, the driver attempts login with FL_PORT (Switched Fabric Loop Port).
	• If FL_PORT login is successful, public loop operation is employed.
	• If FL_PORT login is unsuccessful, private loop mode is entered. If a fabric is not discovered and the topology is arbitrated loop, the driver operates in private loop mode using the following rules:
	  • If an FC-AL device map is present, each node described in the map is logged and verified as a target.
	  • If an FC-AL device map is not present, logins are attempted with all 126 possible FC-AL addresses. LPGO/PRLO are also handled by the driver. Reception of either causes a new discovery or login to take place.
		0

Switched Fabric Operation	• If F_PORT (point-to-point) login is successful, fabric mode is used.
	• If F_PORT login is unsuccessful, N_PORT-to-N_PORT direct connection topology will be used.
	• If a switch is discovered, the driver performs the following tasks:
	  • FL_PORT login (Topology = 0;).
	  • F_PORT login (Topology =1;).
	  • Simple Name Server login.
	  • State Change Registration.
	  • Symbolic Name Registration.
	  • FCP Type Registration if RegFcpType is set to 1.
	  • The driver logs out and re-logs in. The name server indicates that registration is complete.
	  • Simple Name Server Query for devices (the registry parameter SnsAll determines whether all N_Ports are requested (SnsALL=1;) or only SCSI FCP N_Ports (SnsAll=0; default)
	  • Discovery/device creation occurs for each target device described by the Name Server.
	  • The driver handles RSCN and LOGO/PRLO. Reception of either causes new discovery/logins to take place.
		1

*FC-AL attempt first, then attempt point-to-point.	• Topology fail-over requires v3.20 firmware or higher. If firmware does not support topology fail-over, options 0 and 2 are analogous. Options 1 and 3 are analogous.	2
*point-to-point fabric attempt first, then attempt FC-AL.	• Topology fail-over requires v3.20 firmware or higher. If firmware does not support topology, fail-over options 0 and 2 are analogous. Options 1 and 3 are analogous.	3

1: This driver is "Soft-Zone-Safe".
2: In a fabric environment, the order that disk devices are created is based upon the name server response data (which is not guaranteed in any special order). Between successive boots, the same device may be identified with a different physical device number. However, any devices which have been assigned a device letter through disk administrator continue to use that letter regardless of the physical device number.

Setting Topology with HBAnyware

The Driver Parameters tab allows you to change the topology for a single HBA or for all HBAs in one host.

To change topology:

1. Start HBAnyware.
2. In the discovery- tree, click the HBA or the host.
3. Click the Driver Parameters tab.
4. Click the Topology parameter.
5. Select a new value from the drop-down list.
6. Click **Apply**.
7. Reset the HBA to make this change effective.

Setting Topology with lputilnt

To change topology:

1. Select an HBA.
2. Select Driver Parameters from the Category list.
3. Double-click on Topology and the Modify Driver Parameter window is displayed.
4. Enter new topology value in the New Value field and click **Change**.
5. Reset the HBA to make this change effective.

Mapping and Masking

Automapping SCSI Devices

The driver defaults to automatically mapping SCSI devices. The procedures in this section apply if the default has been changed.

Automapping SCSI Devices with HBAnyware

To automap SCSI devices:

1. Start HBAnyware.
2. Display driver parameters for the host or HBA - click the Driver Parameters tab or the Host Driver Parameters tab.
3. Select the AutoMap HBA parameter. Several fields about the parameter appear on the right side of the screen.
4. Select the Enabled radio button.
5. If you want a temporary change (where the parameter reverts to its last permanent setting when the system reboots), check the "Make change temporary" box. This option is available only for dynamic parameters.
6. If you need to make changes to multiple parameters, and you want all the changes temporary, check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be temporary.
7. To apply your changes, click **Apply**.
8. Reboot the system for this change to take effect.

Automapping SCSI Devices with lputilnt

To automap SCIS devices:

1. Start lputilnt.
2. Select an HBA.
3. Select Driver Parameters from the Category list.
4. Double-click on Automap and the Modify Driver Parameter window is displayed:
5. Enter new automap value in the New Value field and click **Change**.
6. Reboot the system for this change to take effect.

Target and LUN Mapping and Masking Using lputilnt

Overviews

Globally Automapping All Targets

Global Automap All Targets defaults to enabled to allow the Emulex driver to detect all FC devices attached to the Emulex HBAs. Global automapping assigns a WWPN, target ID, SCSI bus and SCSI ID to the device. The SCSI bus and SCSI ID may change when the system is rebooted. With persistent binding applied to one of these targets, the SCSI bus and SCSI ID remain the same, whether the system is rebooted or Global Automap All Targets is enabled.

With Global Automap All Targets disabled, the Emulex driver detects FC devices attached to the HBA, and does not pass them to the operating system unless they have already been persistently bound.

Globally Automapping All LUNs

Global Automap All LUNs defaults to enabled and assigns an operating system LUN ID to a FC LUN ID for all LUNs behind the targets in your SAN. LUN mapping can also be enabled and disabled at the target level.

Global automapping of LUNs is different from persistent binding. Global LUN automapping does not concern itself with the SCSI ID or SCSI Bus because the global LUN mapping will stay the same for the target when the system reboots.

Globally Unmasking All LUNS

Globally Unmask All LUNs defaults to enabled, to allow the operating system to see all LUNS behind all targets. If Globally Unmask All LUNs is set to disabled and you want the operating system to see the LUNS behind a specific target, you need to set unmasking at the target level.

Target LUN Automapping

Target LUN automapping defaults to disabled. If enabled, target LUN automapping assigns operating system LUN IDs to a fixed FC target's physical LUNs. Global LUN automapping must be disabled to do target LUN automapping.

Target LUN automapping differs from persistent binding. Persistent binding assigns a WWPN of a FC target device to an operating system target ID, SCSI bus and SCSI ID. The SCSI bus and SCSI ID may change when the system is rebooted. With persistent binding applied to one of these target devices, the SCSI bus and SCSI ID remain the same when the system is rebooted or global target automapping is disabled.

LUN paths are displayed in Disk Manager (when you perform a re-scan) and are displayed dynamically in HBAnyware.

Target LUN Masking

Target LUN masking defaults to disabled. You can mask and unmask LUNs at the target level. If you have unmasked all LUNs for a specific target (either using the global or target functions), you can mask and unmask an individual LUN as well. The HBA can detect all LUNs for the specific target and will present only the unmasked ones.

Mapping and Masking Window Defaults

Table 12 describes LUN mapping and masking global defaults.

Table 12: Mapping and Masking Window Defaults

Field (Function)	Default	Description	Window
Globally Automap All Targets	Enabled	Emulex driver detects all FC devices attached to the Emulex HBAs.	Global Automap
Globally Automap All LUNs	Enabled	Assigns an operating system LUN ID to a FC LUN ID for all LUNs behind all targets in the system area network.	Global Automap
Globally Unmask All LUNs	Enabled	Allows the operating system to see all LUNs behind all targets.	Global Automap
Automap All LUNs (Target Level)	Disabled	With Globally Automap All LUNs disabled, this parameter assigns an operating system LUN ID to a FC LUN ID for all LUNs behind the selected target.	LUN Mapping
LUN Unmasking (Target Level)	Disabled	Allows the operating system to see all LUNs behind the selected target. With this parameter disabled, each individual LUN can be masked or unmasked.	LUN Mapping

Setting Mapping and Masking

The driver defaults to enabling global mapping and masking tasks. The procedures in this section apply if the default has been changed.

Prerequisites

- The SCSIport Miniport driver is properly installed.
- The lputilnt utility is properly installed.
- A target device with LUNs is properly configured.
- For automapping LUNS for a target, the Global Automap All LUNs setting on the Global Automap window is disabled. If necessary, disable this function and reboot the system before automapping LUNS for a target.

Globally Automapping All Targets

Global Automap All Targets defaults to enabled to allow the Emulex driver to detect all FC devices attached to the Emulex HBAs.

To globally automap all targets:

1. Start lputilnt.
2. Select an HBA.
3. Select Persistent Bindings from the Category list.
4. Click **Automap**. The Global Automap window is displayed.
5. Change the Automap All Targets setting to Enabled.
6. Click **OK.** The window closes.
7. Reboot the system for this change to take effect.

Note: With persistent binding applied to one of these targets, the SCSI bus and SCSI ID remain the same when the system is rebooted.

Globally Mapping All LUNs

Global Automap All LUNs defaults to enabled and assigns an operating system LUN ID to a FC LUN ID for all LUNs behind the targets in your SAN. LUN mapping can also be enabled and disabled at the target level.

To globally map all LUNs:

1. Start lputilnt.
2. Select an HBA.
3. Select Persistent Bindings from the Category list.
4. Click **Automap**. The Global Automap window is displayed.
5. Change the Globally Automap All LUNs setting to Enabled.
6. Click **OK**. The window closes.
7. Reboot the system for this change to take effect.

Globally Unmasking or Masking All LUNs

Globally Unmask All LUNs defaults to allow the operating system to see all LUNs behind targets.

To globally unmask or mask all LUNS:

1. Start lputilnt.
2. Select an HBA.
3. Select Persistent Bindings from the Category list.
4. Click **Automap**. The Global Automap window is displayed.
5. Change the Unmask All LUNs setting to Enabled.
6. Click **OK**. The window closes.

This change takes effect without a reboot.

Automapping LUNs for a Target

Target LUN Automapping defaults to disabled. If enabled, target LUN automapping assigns an operating system LUN ID to a fixed FC target's physical LUN.

To automap LUNs for a target:

1. Start lputilnt.
2. Select an HBA.
3. Select Persistent Bindings from the Category list. All targets are displayed.
4. Click on a target. The **Lunmap** button becomes active.
5. Click **Lunmap**. The LUN Mapping window is displayed.
6. Change the LUN Automap function to Enabled. Target automapping assignment occurs and these assignments are displayed on the LUN Mapping window.
7. Click **OK**.
8. Reboot the system for this change to take effect.

LUN Masking and Unmasking for a Target

Target LUN Automapping defaults to disabled. If enabled, target LUN automapping assigns operating system LUN IDs to a fixed FC target's physical LUNs. Global LUN automapping must be disabled for target LUN automapping.

To unmask or mask a LUN:

1. Start lputilnt.
2. Select an HBA.
3. Select Persistent Bindings from the Category list. All targets are displayed.
4. Click on a target. The **Lunmap** button becomes active.
5. Click **Lunmap**. The LUN Mapping window is displayed. All LUNs are displayed for the target.
6. Do the following:
   - To unmask or mask all LUNs for the target, set the LUN Unmasking function to Disabled.
   - To mask or unmask a LUN, select the row and click **Edit**. In the Edit Map Entry area, click on the Mask (Unmask) field to change the status.

   Note: If LUNs are not displayed, LUN mapping has been disabled at the global level and not enabled at the target level, or the LUNs have been masked at the global level.
7. Click **OK**.

   These changes do not require a reboot.

Setting Up Persistent Binding

Global automapping assigns a binding type, target ID, SCSI bus and SCSI ID to the device. The binding type, SCSI bus and SCSI ID may change when the system is rebooted. With persistent binding applied to one of these targets, the WWPN, SCSI bus and SCSI ID remain the same, whether the system is rebooted or with Global Automap All Targets subsequently disabled (enabled by default). The binding information is permanent because it is stored in the Windows registry. The driver refers to the binding information at bootup.

Persistent binding permanently maps a device to the following:

- Binding type
- SCSI bus
- SCSI ID

You can set up persistent binding using HBAnyware or lputilnt.

- HBAnyware allows you to set up persistent binding on remote and local HBAs.
- lputilnt allows you to set up persistent binding on local HBAs only.

Setting Up Persistent Binding with HBAnyware

To set up persistent binding:

1. Start HBAnyware.
2. In the discovery-tree, click the HBA you want to set up with persistent binding.

3. Click the **Target Mapping** tab. All targets are displayed.

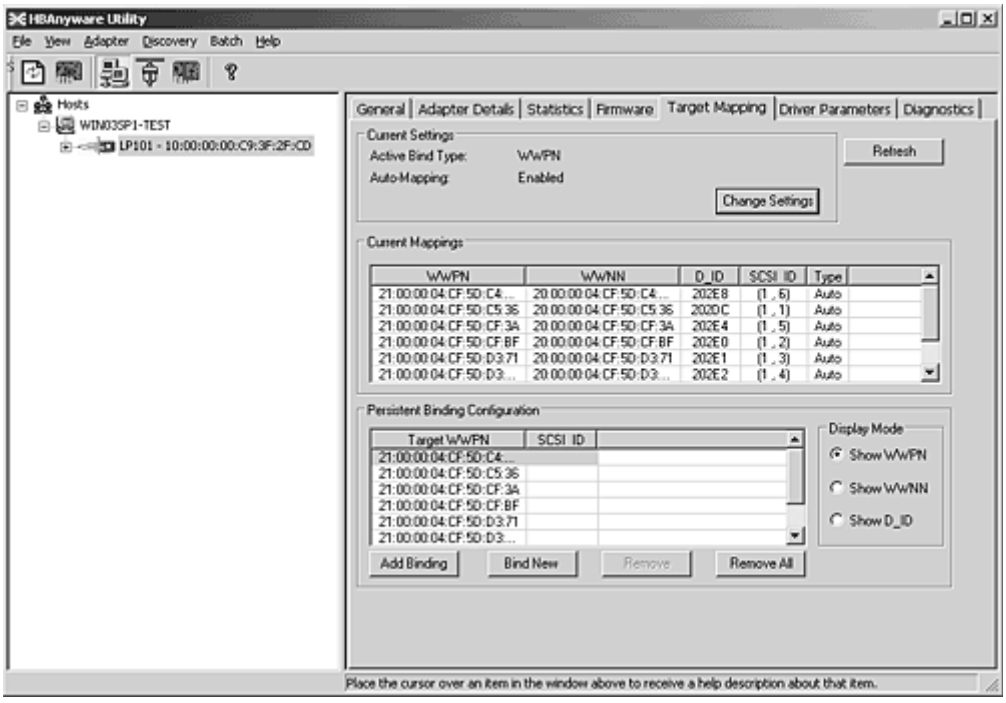

Figure 37: HBAnyware Utility, Target Mapping Tab

4. Target mappings are displayed by WWPN, WWNN, or D_ID. “PB”, indicates mapping from persistent binding, while “Auto”, indicates an automapped target. In the Display Mode section, choose the display mode you want to use.
5. **Change Setting** - click to change the active bind type (the mode used to persistently bind target mappings), LUN automapping or LUN unmasking settings. Select the active bind type (WWPN, WWNN or D_ID), enable or disable LUN automapping nd/or set enable or disable LUN unmasking.

To add a persistent binding:

1. In the Targets Table, click the target that you want to bind.
2. Click **Add Binding**. The Add Persistent Binding dialog box is displayed.

Figure 38: HBAnyware, Utility, Add Persistent Binding Dialog Box

3. Select the bind type that you want to use (WWPN, WWNN or D_ID).

4. Select the bus ID and target ID that you want to bind, and click **OK**.

Note: Automapped targets will have entries only in the second column of the Targets Table. Persistently bound targets will have entries in the second and third columns. In this case, the third column contains the SCSI bus and target numbers you specified in the Add Persistent Binding dialog box. This binding will take effect only after the local machine is rebooted.It is possible to specify a SCSI bus and target that have already been used on behalf of a different FC target. HBAnyware does not detect this until you click the **OK** button in the Add Persistent Binding dialog box. Then a "duplicate binding" error message is displayed, and the request is rejected.

To bind a target that does not appear in the Persistent Binding table on the Target Mapping tab:

Note: Attempting to bind a target already in the Persistent Binding table on the Target Mapping tab results in an error message, “Target already in target list. Use the Add Binding button.”

1. Click **Bind New**. The **Bind New Target** dialog box is displayed.

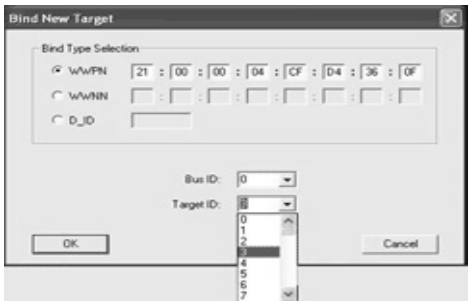

Figure 39: HBAnyware Utility, Bind New Target Dialog Box

2. Click the type of binding you want to use, and type the WWPN, WWNN or D_ID you want to bind to the target.
3. Select the Bus ID and Target ID that you want to bind, and click **OK**.

Note: A target will not appear on the target list if automapping has been disabled and the target is not already persistently bound.

Setting Up Persistent Binding with lputilnt

To perform binding tasks:

1. Start lputilnt.
2. Select an HBA.

3. Select Persistent Bindings from the Category list. All targets are displayed.

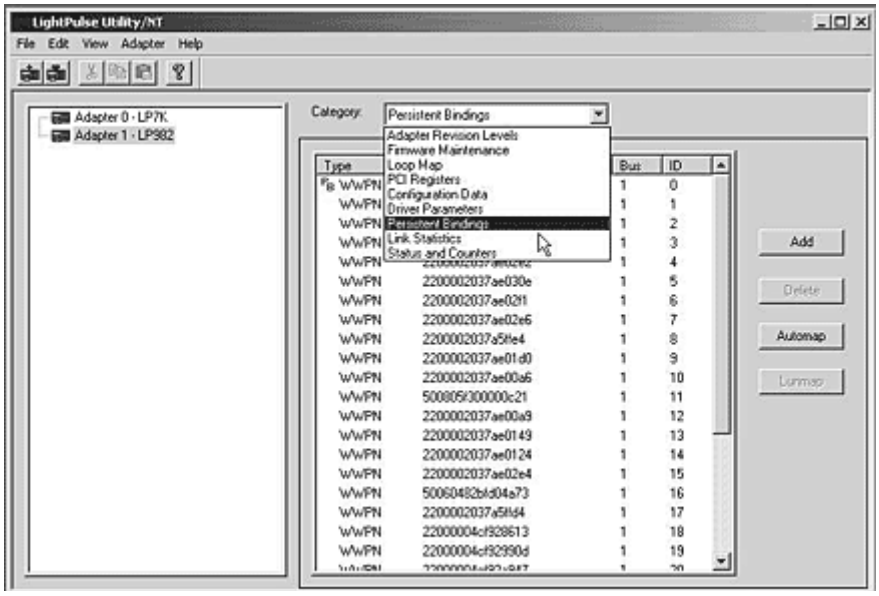

Figure 40: lputilnt Utility, Persistent Bindings Category

4. Click on a target and click **Add**. The Add Binding window is displayed.

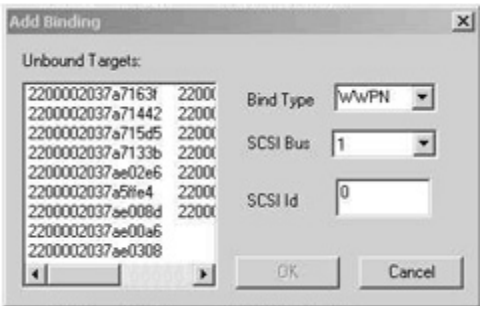

Figure 41: lputilnt Utility, Add Binding Window

5. In the Add Binding window, click the target you want to bind in the Unbound Targets list.
    - The bind type is controlled by two driver parameters: Hard Address and MapNodename. These parameters can be changed using the Driver Parameters window. HardAddress - this parameter controls whether the driver maps addresses based on WWPN, a fixed FC-AL hard address or a fabric D_ID.
        - If set to 0 (default), the driver maps bus/target addresses by WWPN.
        - If set to 1, the driver maps bus/target addresses to fixed FC-AL hard address or fabric D_ID (some hot swap applications can require HardAddress=1).
    - MapNodeName - this parameter controls whether the SCSIport Miniport driver maps and tracks devices based on WWPN or nodename. The HardAddress parameter must be set to 0 for the MapNodeName parameter to be active.
        - If set to 0 (default), the driver maps and tracks devices based on WWPN.
        - If set to 1, the driver maps and tracks devices base on Nodename.

    See “Setting Parameters Using lputilnt” on page 73 for information on how to set these driver parameters.
6. If necessary, change the SCSI Bus and SCSI ID values.

7. Click **OK** to bind the target.The letters "PB" will be displayed next to the target row.

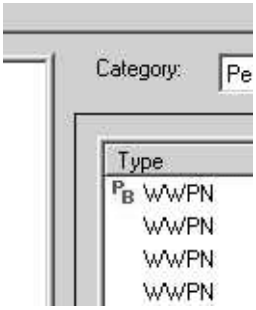

Figure 42: Persistent Binding Designation for Targets

8. Reboot the system for these changes to take effect.
9. Start lputilnt. Your new device and SCSI ID mapping information is displayed in the SCSI Target List area.

Updating Firmware or Boot Code

You can update firmware or boot code with either HBAnyware or lputilnt.

- HBAnyware allows you to update firmware or boot code on remote and local HBAs.
- lputilnt allows you to update firmware or boot code on local HBAs only.

Updating Firmware or Boot Code with HBAnyware

Prerequisites

- The SCSIport Miniport driver is properly installed.
- The HBAnyware utility is properly installed.
- The firmware or boot code file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.

Procedure

To update firmware or boot code:

1. Start the HBAnyware utility (see page 24).
2. In the discovery-tree (left pane), click the HBA where you want to update the firmware or boot code.

3. In the property tabs (right pane), select the Firmware tab.

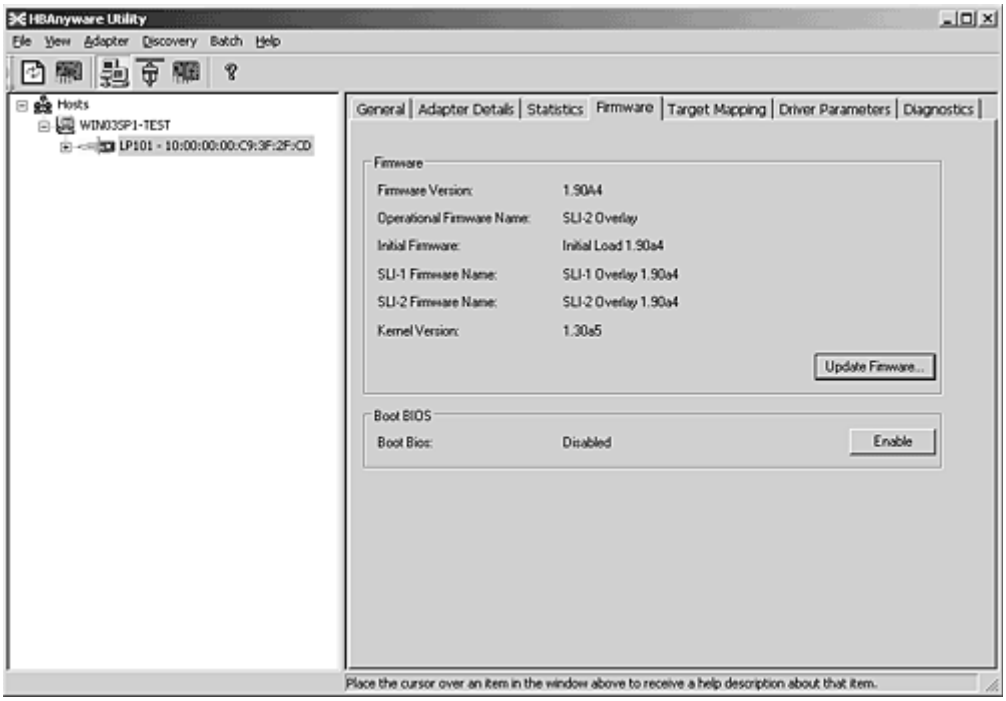

Figure 43: HBAnyware Utility, Firmware Tab (Example)

4. Click **Update Firmware**. The adapter reset notice appears. Click **Yes**.

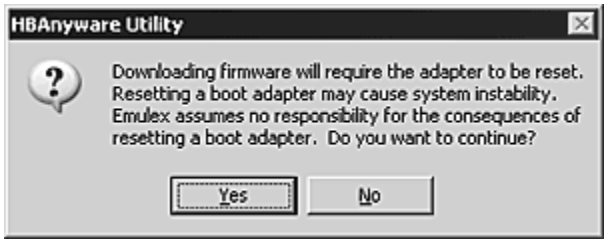
HBAnyware Utility
Downloading firmware will require the adapter to be reset. Resetting a boot adapter may cause system instability. Emulex assumes no responsibility for the consequences of resetting a boot adapter. Do you want to continue?
Yes
No

Figure 44: HBAnyware Utility, Adapter Reset Notice

5. Click **Yes.** The Firmware Download dialog box appears:

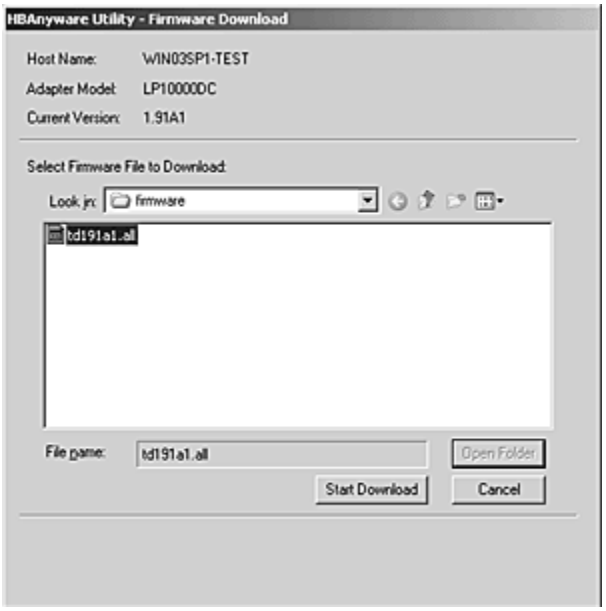

Figure 45: HBAnyware Utility, Firmware Download Dialog Box (Example)

6. Navigate to the extracted firmware or boot code file you wish to download:
   - Firmware files have an .all extension.
   - Boot code files have a .prg extension.
7. Select the firmware or boot code file and click **Start Download**. A status bar shows the progress of the download and indicates when the download has completed.
8. Click **Close**. The Firmware tab shows the updated firmware or boot code information for the selected HBA.

   If you are updating firmware or boot code on a dual-channel HBA, repeat steps 2 - 9 to update the firmware or boot code on a second port.

Note: Step 10 – 12 apply only to x86 BootBIOS. For EFIBoot, you must enable the boot code using the EFI utility; see the EFIBoot documentation for more information.

9. Enable the boot code. If the boot code is already enabled (on the Firmware tab, the Boot Bios button title is **Disable** – see Figure 25), skip to step 12. Otherwise, continue with step 11.
10. Click **Enable**. The button title changes from **Enable** to **Disable**.

Note: If the state of the boot code has changed, this change is reflected immediately on the General tab.

11. If you are updating x86 BootBIOS, you must also enable the HBA to boot from SAN using the BIOS utility; see the documentation that accompanies the boot code for more information.

Updating Firmware or Boot Code (Batch Mode) with HBAnyware

Loading firmware or boot code in batch mode enables you to install firmware or boot code on multiple HBAs in a single step. Batch firmware or boot code loading is restricted to a single firmware or boot code file and to all accessible HBAs for which that file is compatible.

Note: No other HBAnyware functions can be performed while batch firmware or boot code loading is in progress.

Prerequisites

- TheSCSIport Miniport driver is properly installed.
- The HBAnyware utility is properly installed.
- The firmware or boot code file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.

Procedure

To update firmware or boot code in batch mode:

1. Start the HBAnyware utility(see page 24).
2. From the menu, select Batch and click Download Firmware. The Select Firmware File dialog box appears.

Note: You do not need to select a particular tree element for this operation.

3. Navigate to the extracted file you want to download. Select the file and click **Open**. A tree-view shows all HBAs and their corresponding hosts that are compatible with the selected firmware or boot code file.

Figure 46: HBAnyware Utility, Selecting HBAs to Update (Example)

4. Click the box next to an HBA to select or remove the HBA from the batch process.Click the box next to a host to select or remove all eligible HBAs for the host from the batch process.
5. Click **Start Download**.

6. File downloading begins and the tree-view displays the progress. As the file for a selected HBA is being downloaded, it appears orange in the tree-view. When the download is finished, the entry changes to green (Figure 47). If the download failed, the entry changes to red.

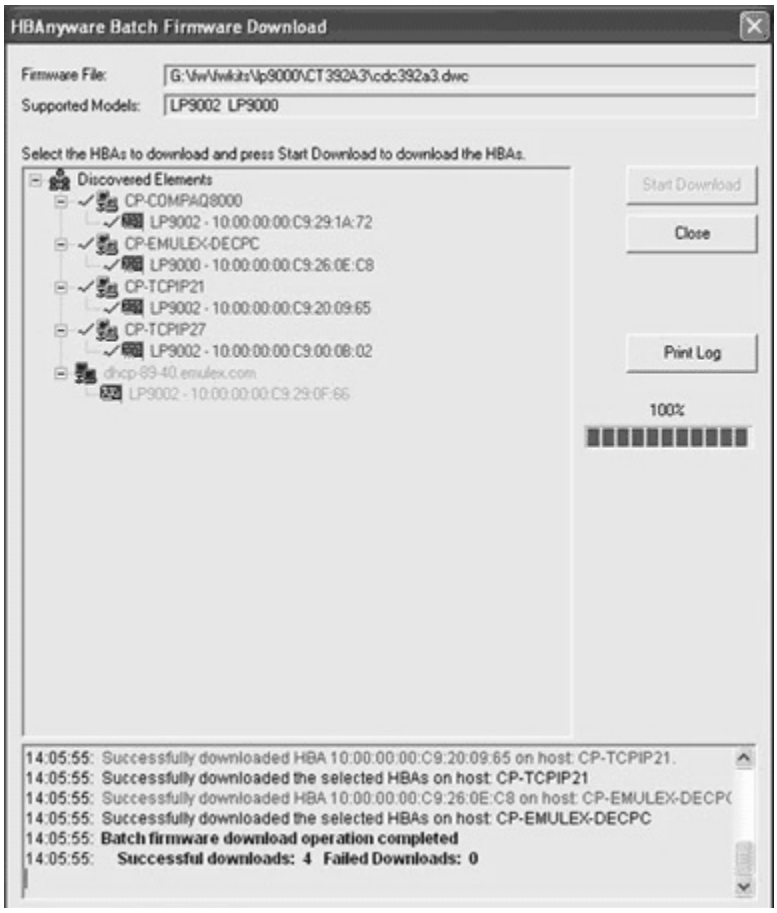

Figure 47: HBAnyware Batch Firmware Download Window, Download Complete

7. When downloading is finished, click **Print Log** for a hard copy of the activity log.
8. Click **Close** to exit the batch procedure.

Updating Firmware or Boot Code with lputilnt

Prerequisites

- The SCSIport Miniport driver is properly installed.
- The lputilnt utility is properly installed.
- The firmware or boot code file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.
- The system is in a state safe in which this type of maintenance can be performed:
  - I/O activity on the bus has been quieted.
  - Cluster software, or any other software that relies on the HBA to be available, has been stopped or paused.

Caution: Firmware or boot code versions differ between HBA models. Make sure you have downloaded the appropriate firmware or boot code for your HBA.

Procedure

Note: No other functions can be performed while firmware or boot code loading is in progress.

To update firmware or boot code:

1. Start lputilnt (see page 48).
2. Select the desired HBA.
3. Select Firmware Maintenance from the Category list.

Note: If the letter W appears next to a firmware entry, the image is represented in the wakeup parameters. This means that the HBA will use that specific image if it needs a firmware image.

4. Click **Download**.
5. Locate the new firmware or boot code file.
6. Click **Open**.
7. File downloading begins.

   If you are updating firmware or boot code on a dual-channel HBA, repeat steps 2 - 6 to update the firmware or boot code on a second port.
8. If you are updating boot code, you must also enable the HBA to boot from SAN using the BIOS utility; see the documentation that accompanies the boot code for more information.

Performing Basic Diagnostic Tests with HBAnyware

Use the Diagnostics tab to do the following:

- Run these tests on Emulex HBA's installed in the system:
  - PCI Loopback (see page 112)
  - Internal Loopback (see page 112)
  - External Loopback (see page 112)
  - Power-On Self Test (POST) (see page 109)
  - Echo (End-to-End) (see page 114)
  - Quick Test (see page 108)
- Perform a diagnostic dump (see page 110).
- View PCI registers and wakeup parameter (see page 111).
- Control HBA beaconing (see page 110).

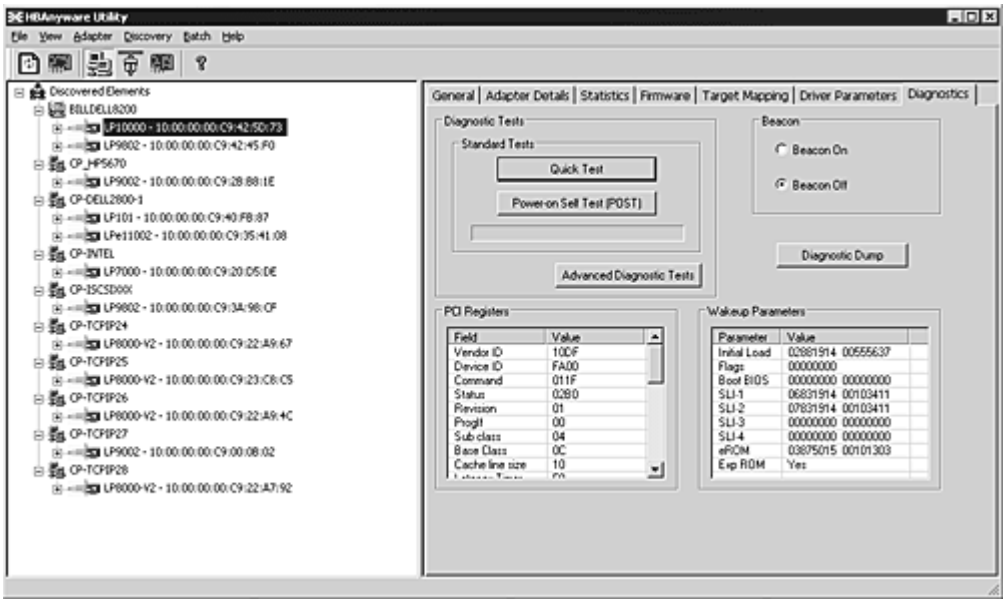

Figure 48: HBAnyware Utility, Diagnostics Tab

All functions are supported locally and remotely, except for the dump feature which is only supported locally.

Running a Quick Test

The Diagnostics tab enables you to run a "quick" diagnostics test on a selected HBA. The Quick Test consists of 50 PCI Loopback test cycles and 50 Internal Loopback test cycles.

To run a quick test:

1. Start HBAnyware.
2. From the discovery-tree, select the HBA on which you wish to run the Quick Test.

3. Select the Diagnostics tab and click **Quick Test**. The following message appears:

HBAnyware Utility
Running the Quick test will result in taking the selected adapter off line.
Ensure that all IO activity on this port has stopped before proceeding.
Click OK to run the test, or Cancel to skip it
OK
Cancel

Figure 49: HBAnyware Utility, Quick Test Message

4. Click **OK** to run the test. The Quick Diagnostics Test message shows the PCI Loopback and Internal Loopback test results.

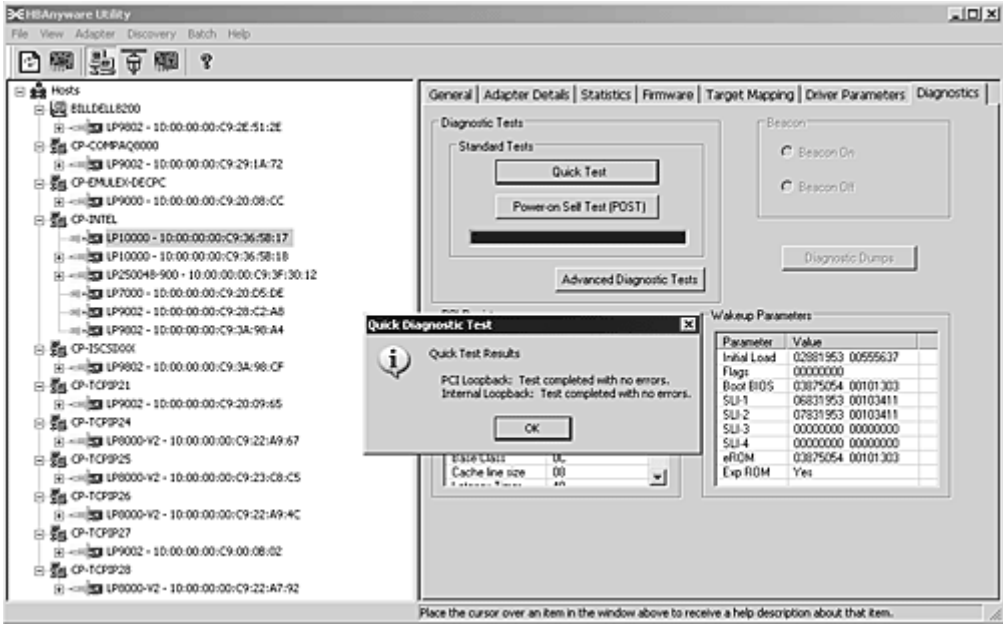

Figure 50: HBAnyware Utility, Quick Diagnostics Test Results

Running a POST Test

The POST (Power On Self Test) is a firmware test normally performed on an HBA after a reset or restart. The POST does not require any configuration to run.

To run the POST Test:

1. Start HBAnyware.
2. From the discovery-tree, select the HBA on which you wish to run the POST Test.
3. Select the Diagnostics tab and click **Power-on Self Test (POST)**. A warning dialog box appears (see Figure 50).
4. Click **OK**. A POST Test window shows POST test information.

Figure 51: HBAnyware Utility, POST Test Window

Using Beaconing

The beaconing feature enables you to force a specific HBA's LEDs to blink in a particular sequence. The blinking pattern acts as a beacon, making it easier to locate a specific HBA among racks of other HBAs.

When you enable beaconing, the two LEDs blink rapidly in unison for 24 seconds, after which the LEDs report the HBA health status for 8 seconds. When the 8 seconds are up, the HBA returns to beaconing mode. This cycle repeats indefinitely until you disable this feature or you reset the HBA.

Note: The beaconing buttons are disabled if the selected HBA does not support beaconing.

To enable/disable beaconing:

1. Start HBAnyware.
2. From the discovery-tree, select the HBA whose LEDs you wish to set.
3. Select the Diagnostics tab and click **Beacon On** or **Beacon Off**.

Starting a Diagnostic Dump

Note: The Diagnostic Dump feature is only supported for local HBAs. If a remote HBA is selected from the tree-view, the Initiate Diagnostic Dump is disabled.

To start a diagnostic dump:

1. Start HBAnyware.
2. From the discovery-tree, select a local HBA whose diagnostic information you want to dump.
3. Select the Diagnostics tab and click **Diagnostic Dumps**. The Diagnostic Dump dialog box appears. You can specify how many files you want to save using the Files Retained counter. Click **Delete Existing Dump Files** if you wish to remove existing dump files from your system.

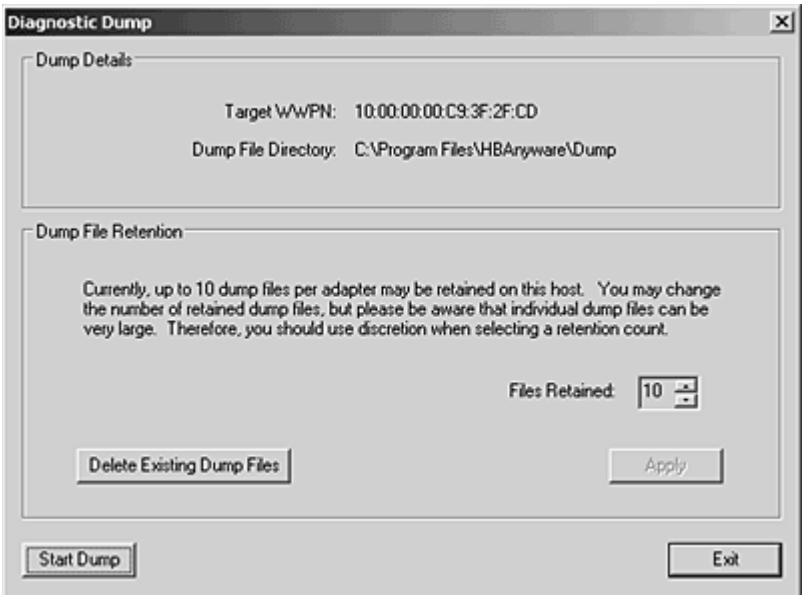
Diagnostic Dump
Dump Details
Target WWPN: 10:00:00:00:C9:3F:2F:CD
Dump File Directory: C:\Program Files\HBAnyware\Dump
Dump File Retention
Currently, up to 10 dump files per adapter may be retained on this host. You may change the number of retained dump files, but please be aware that individual dump files can be very large. Therefore, you should use discretion when selecting a retention count.
Files Retained: 10
Delete Existing Dump Files
Apply
Start Dump
Exit

Figure 52: HBAnyware Utility, Diagnostic Dump Dialog Box

4. Click **Start Dump**.

Displaying PCI Registers and Wakeup Information

A PCI Register dump for the selected HBA appears in the lower left panel of the Diagnostics tab. Wakeup information for the selected HBA appears in the lower right panel of the Diagnostics tab. The information is read-only and is depicted below:

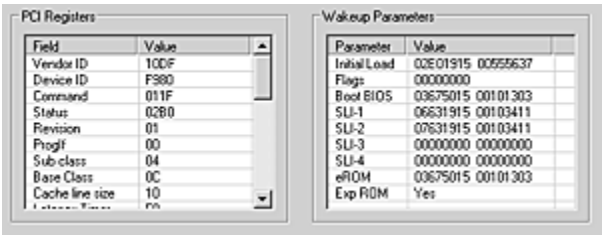

Figure 53: HBAnyware Utility, PCI Registers and Wakeup Parameters Area of the Diagnostics Tab

Running Advanced Diagnostic Tests with HBAnyware

The Advanced Diagnostics feature gives you greater control than the Quick Test over the type of diagnostics tests that run. Through Advanced Diagnostics, you can specify which tests to run, the number of cycles to run, and what to do in the event of a test failure.

To run advanced diagnostics tests:

1. Start HBAnyware.
2. Click **Advanced Diagnostics Test** on the Diagnostics tab to view the Advanced Diagnostics dialog box.

   You can run four types of tests:

   - PCI Loopback
   - Internal Loopback
   - External Loopback
   - End-to-End (ECHO)

Note: You cannot run the External Loopback test and ECHO test concurrently. If you select External Loopback the ECHO test section is disabled and vice versa.

All test results, plus the status of running tests, are time stamped and appear in the log at bottom of the dialog box.

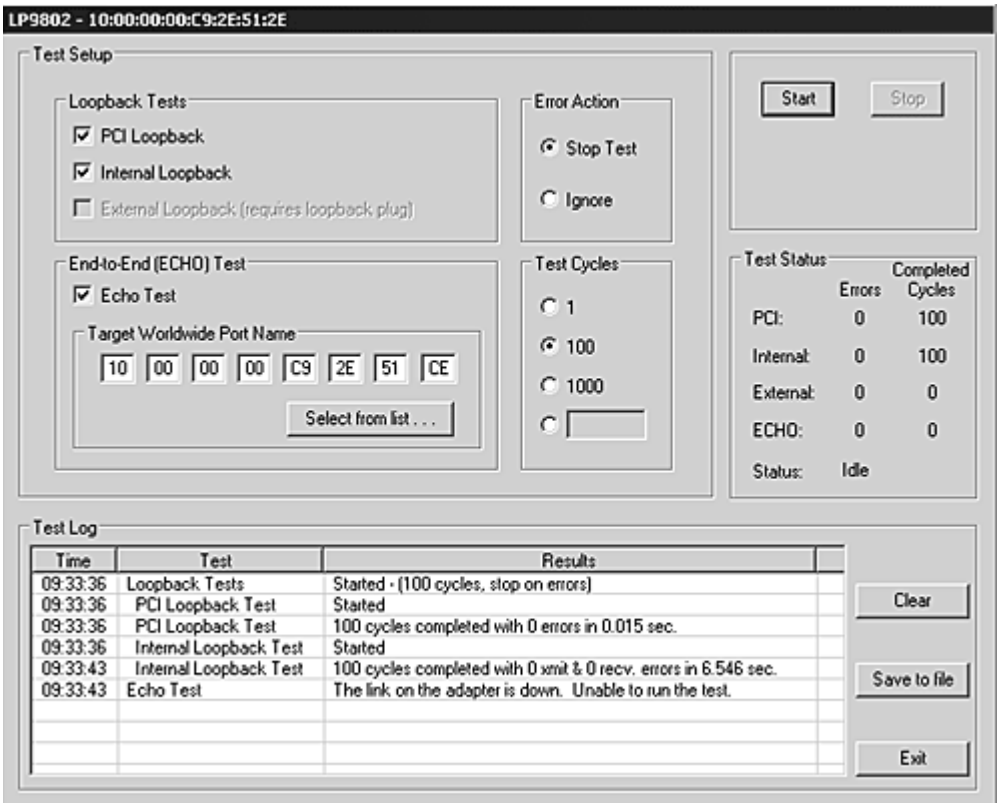

Figure 54: HBAnyware Utility, Advanced Diagnostics

Running Loopback Tests

To run a loopback test, use the "Loopback Test" section of the Advanced Diagnostics dialog box.

You can run the following loopback test combinations using the appropriate boxes:

- PCI Loopback Test - A firmware controlled diagnostic test in which a random data pattern is routed through the PCI bus without being sent to an adapter link port. The returned data is subsequently validated for integrity.
- Internal Loopback Test - A diagnostic test in which a random data pattern is sent down to an adapter link port, then is immediately returned without actually going out on the port. The returned data is subsequently validated for integrity.
- External Loopback Test - A diagnostic test in which a random data pattern is sent down to an adapter link port. The data goes out the port and immediately returns via a loopback connector. The returned data is subsequently validated for integrity.

Note: You cannot run the External Loopback test and ECHO test concurrently. If you select External Loopback the ECHO test section is disabled and vice versa.

You can specify the number of test cycles by clicking one of the cycle counts values in the "Test Cycles" section of the dialog box or enter a custom cycle count if you wish. The Test Status section displays how many cycles of each test ran. The "Error Action" section of the dialog box enables you to define what should be done in the event of a test failure.

There are two error action options:

- Stop Test - The error will be logged and the test aborted. No further tests will run.
- Ignore - Log the error and proceed with the next test cycle.

To run loopback tests:

1. Start HBAnyware.
2. From the discovery-tree, select the HBA on which you wish to run the Loopback Test.
3. Select the Diagnostics tab and click **Advanced Diagnostics Tests**. From the Loopback Test section of the dialog box, choose the type of Loopback test you wish to run and define the loopback test parameters.

   Note: You must insert a loopback plug in the selected HBA before running an External Loopback test.

4. Click **Start**. The following warning appears:

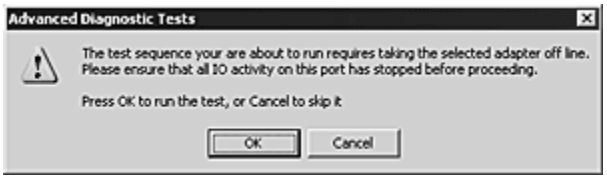
Advanced Diagnostic Tests
The test sequence your are about to run requires taking the selected adapter off line. Please ensure that all IO activity on this port has stopped before proceeding.
Press OK to run the test, or Cancel to skip it
OK
Cancel

Figure 55: HBAnyware Utility, Advanced Diagnostic Tests Warning

5. Click **OK**. If you choose to run an External Loopback test the following window appears:

Advanced Diagnostic Tests
The test sequence your are about to run requires taking the selected adapter off line. Please ensure that all IO activity on this port has stopped before proceeding.
The loopback tests you have chosen require that a loopback plug be inserted into the back of the adapter to be tested. Failure to do so can result in the board not returning to an on line state. Please make sure the loopback plug is inserted before pressing the OK button.
Press OK to run the test, or Cancel to skip it
OK
Cancel

Figure 56: HBAnyware Utility, Advanced Diagnostic Tests Warning for External Loopback

6. Click **OK**. The progress bar indicates that the test is running.

   Periodic test feedback, consisting of the current loopback test/cycle plus the completion status of each type of test, is displayed in the "Test Log" section of the dialog box. Click **Clear** to erase the contents of the log display or click **Save** to File to save the log file.

Running End-to-End (ECHO) Tests

Run echo tests using the "End-to-End (ECHO) Test" section of the Diagnostics tab. The end-to-end test enables you send an ECHO command/response sequence between an HBA port and a target port.

Note: Not all remote devices respond to an echo command.

You cannot run the ECHO test and the External Loopback test concurrently. If you select the ECHO Test the External Loopback test is disabled.

To run end-to-end echo tests:

1. Start HBAnyware.
2. From the discovery-tree, select the HBA from which you wish to initiate the End-to-End (ECHO) Test.
3. Select the **Diagnostics** tab. Click **Advanced Diagnostics Test**.
4. Do one of the following:
   - Check **Echo Test**. Enter the World Wide Port Name (WWPN) for the target.
   - Click **Select From List** if you do not know the actual WWPN of the test target. The **Select Echo Test Target** dialog box appears. Select the port you wish to test from the tree-view and click **Select**.

   All relevant information for the selected port is automatically added to the Target Identifier section of the **Diagnostics** dialog box.

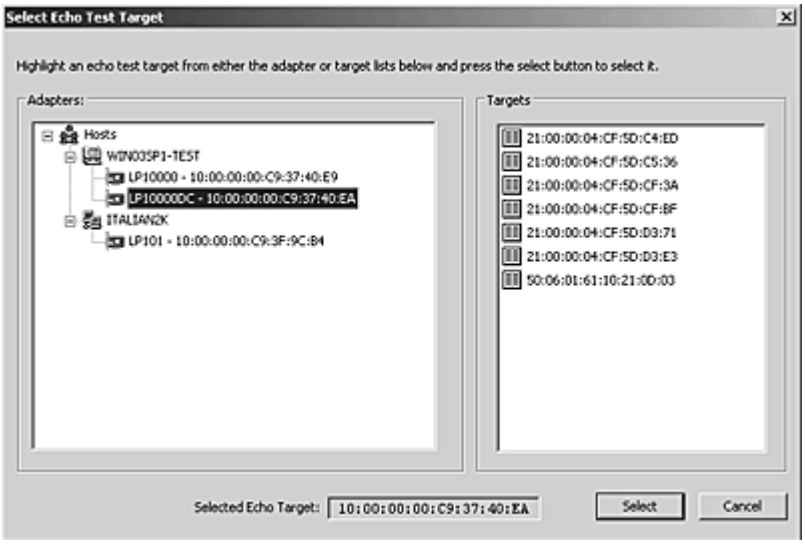

Figure 57: HBAnyware Utility, Select Echo Test Target Window

5. Click **Start**. The following warning window appears:

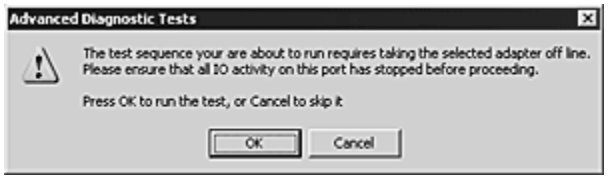
Advanced Diagnostic Tests
The test sequence your are about to run requires taking the selected adapter off line.
Please ensure that all IO activity on this port has stopped before proceeding.
Press OK to run the test, or Cancel to skip it
OK
Cancel

Figure 58: HBAnyware Utility, Advanced Diagnostic Tests Warning

6. Click **OK**. A result screen appears and the test results appear in the Test Log. Click **Clear** to erase the contents of the log display or click **Save to File** to save the log file.

Saving the Log File

You can save the test log to a log file for later viewing or printing. When new data is written to a saved file, the data is appended to the end of the file. Each entry has a two-line header that contains the identifier of the HBA being tested and the date and time of the test. Over time, the data accumulates to forms a chronological history of the diagnostics performed on the HBA.

After writing an entry into the log, you are prompted to clear the display.

The default name of the saved file is DiagTestLog.log and the default location is: PROGRAM_FILES\HBAnyware\Emulex Repository.

An example of a saved log file appears below:

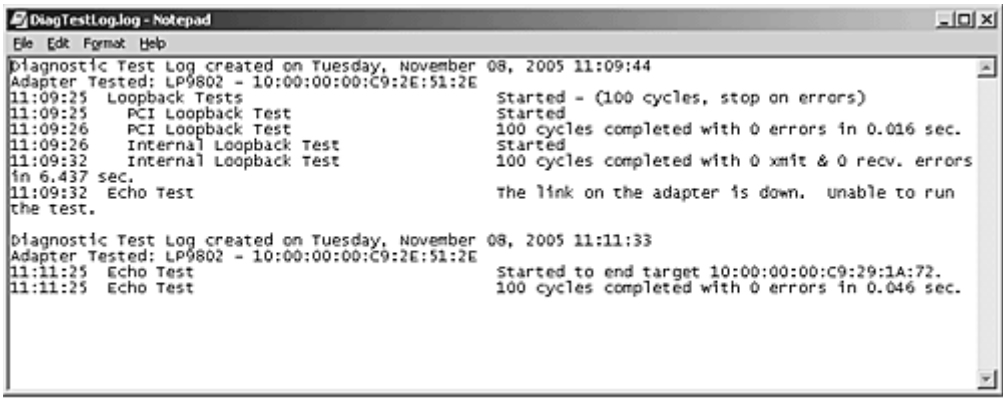
DiagTestLog.log - Notepad
File Edit Format Help
Diagnostic Test Log created on Tuesday, November 08, 2005 11:09:44
Adapter Tested: LP9802 - 10:00:00:00:C9:2E:51:2E
11:09:25 Loopback Tests Started - (100 cycles, stop on errors)
11:09:25 PCI Loopback Test Started
11:09:26 PCI Loopback Test 100 cycles completed with 0 errors in 0.016 sec.
11:09:26 Internal Loopback Test Started
11:09:32 Internal Loopback Test 100 cycles completed with 0 xmit & 0 recv. errors in 6.437 sec.
11:09:32 Echo Test The link on the adapter is down. Unable to run the test.
Diagnostic Test Log created on Tuesday, November 08, 2005 11:11:33
Adapter Tested: LP9802 - 10:00:00:00:C9:2E:51:2E
11:11:25 Echo Test Started to end target 10:00:00:00:C9:29:1A:72.
11:11:25 Echo Test 100 cycles completed with 0 errors in 0.046 sec.

Figure 59: Diag Testlog Window

To save the log file:

1. After running a test from the Diagnostic Test Setup dialog box, Click **Save to File**. The Select Diagnostic Log file Name dialog box appears. The default name of a saved file is DiagTestLog.log.
2. Browse to the desired directory, change the log file name if you wish and click **Save**.

Out-of-Band SAN Management

Out-of-Band (OOB) remote SAN management is achieved by sending the remote management requests over a LAN using the Ethernet TCP/IP protocol to remote hosts.

In-Band management is achieved by sending the remote management requests over a LAN using the FC protocol to remote hosts.

Principle differences between In-Band and Out-of-Band SAN Management:

- A management host with an HBA installed does not need to connect to a fabric to manage other hosts.
- An OOB management host can manage all of the HBAs in a remote host, not just the ones connected to the same fabric. In-band can only manage HBAs connected to the same fabric.
- You can manage many more hosts since OOB is not constrained by the boundaries of a fabric or zoning.
- True board status (e.g. link down) is available since the in-band path is not necessary to send a status request to the remote host.
- HBA security in an OOB environment is much more important since many more hosts are available for management and OOB access is not affected by fabrics or zoning.
- Discovery of hosts in an OOB environment is much more difficult than in-band discovery.
- A host may be able to manage a remote host by sending management requests either in-band or out-of-band.

Adding a Single Host

HBAnyware enables you to specify a single OOB host to manage. If the host is successfully discovered as a manageable host, it is added to the static list of hosts and if it has not been discovered in-band, the host and its HBAs are added to the discovery-tree.

To add a single host:

1. Start HBAnyware.
2. From the Discovery menu, select Out-of-Band/Add Host. The Add Remote Host dialog box appears.

Figure 60: HBAnyware Utility, Add Remote Host Dialog Box

3. Enter the name or the IP address of the host to be added. Entering the IP address is the best way to add a new host.

Note: Entering the host's name will not always work. It requires that there be a DNS server available on the network to resolve the host's name to an IP address. This method will also not work for multi-byte character sets as the system call to resolve the host's name only takes single-byte character sets. If the host's name cannot be resolved, you receive an error message.

4. Click **OK**. If the new host was added successfully you will receive a message indicating this. If the new host could not be added you will receive a message to that effect.

Adding a Range of Hosts

You can find the OOB manageable hosts by searching a range of IP addresses using the Add Remote Hosts dialog box.

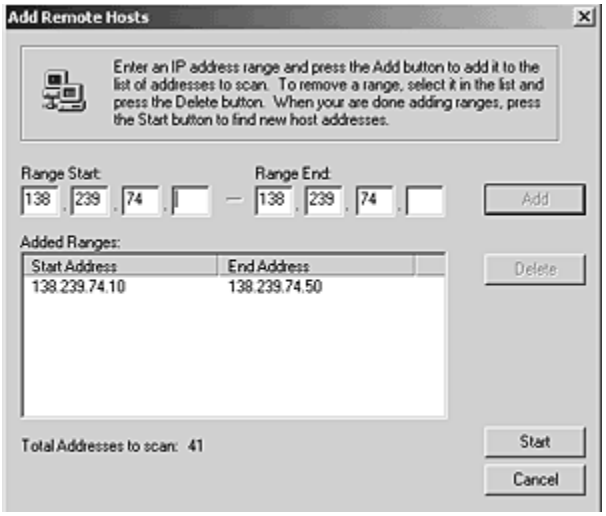
Add Remote Hosts
Enter an IP address range and press the Add button to add it to the list of addresses to scan. To remove a range, select it in the list and press the Delete button. When your are done adding ranges, press the Start button to find new host addresses.
Range Start:
138 . 239 . 74 .
Range End:
138 . 239 . 74 .
Add
Added Ranges:
Start Address
End Address
138.239.74.10
138.239.74.50
Delete
Total Addresses to scan: 41
Start
Cancel

Figure 61: HBAnyware Utility, Add Remote Hosts Window

The Add Remote Hosts dialog box enables you to build the initial list of OOB manageable hosts.

To add a range of hosts:

1. Start HBAnyware.
2. From the Discovery menu, select Out-of-Band/Add Range of Hosts. The Add Remote Hosts dialog box appears. Notice that part of the range start and range end addresses are already filled in based upon the IP address and subnet mask of the management host.
3. Enter the complete start and end address range and click **Add**. The added address range appears in the dialog box. Add any additional ranges you wish to search.
4. Click **Start**. HBAnyware checks each address in the range to determine if the host is available and remotely manageable. The number of addresses discovered (of manageable hosts) is periodically updated on the dialog box.

   Note: The number of addresses does not correspond directly to the number of hosts added to the discovery-tree. Some of the addresses discovered may be for hosts that have already been discovered in-band. However, new HBAs may be discovered on those hosts that were not discovered in-band. A host may have more than one HBA installed and both IP addresses for that host are discovered during the search, but only one host will possibly be added to the discovery-tree.

5. When the search is complete, click **Close**.
6. A dialog box appears asking to save the IP ranges you searched. Click **Yes** to save the address ranges. If you save the address ranges, these address ranges will appear the next time you use the Add Remote Hosts dialog box. Click **No** if you do not want to save the address ranges.

Removing Hosts

Periodically you may want to remove hosts that are no longer part of the network. You may want to remove a host when it is removed from the network or to detect hosts that are no longer being discovered. Removing hosts that can no longer be discovered improves the operation of the discovery server.

To remove hosts:

1. Start HBAnyware.
2. From the Discovery menu, select Out-of-Band/Remove Host. The Remove Remote Hosts dialog box shows a list of discovered OOB hosts. Any host not currently discovered appears in red. Click **Show Undiscovered Hosts Only** to only display currently undiscovered hosts.
3. From the Remove Remote Hosts dialog box, select the hosts you wish to remove. You can select all the displayed hosts by clicking **Select All**.
4. Click **OK** to remove the selected hosts.

HBAnyware Security

Introduction

After you install the base HBAnyware software, which includes the HBAnyware utility and remote server, on a group of systems, the HBAnyware utility on any of those systems can remotely access and manage the HBAs on any systems in the group. This may not be a desirable situation, because any system can perform actions such as resetting boards or downloading firmware.

You can use the HBAnyware security package to control which HBAnyware systems can remotely access and manage HBAs on other systems in a Fibre Channel network. HBAnyware security is systems-based, not user-based. Anyone with access to a system that has been granted HBAnyware client access to remote HBAs can manage those HBAs. Any unsecured system is still remotely accessible by the HBAnyware client software (HBAnyware utility).

The HBAnyware security software provides two main security features:

1. Prevent remote HBA management from systems that you do not want to have this capability.
2. Prevent an accidental operation (such as firmware download) on a remote HBA. In this case, you do not want to have access to HBAs in systems you are not responsible for maintaining.

The first time you run the HBAnyware Security Configurator on a system in an environment where no security as been configured, the initial Access Control Group (ACG) is created. At this point, only this system has remote access to the HBAs in the systems in the ACG. They are no longer remotely accessible from any other system.

Subsequently, you can create additional Access Sub-Groups (ASGs). This grants systems in the ACG the ability to remotely access the HBAs of other selected systems in the ACG.

Starting the HBAnyware Security Configurator

Prerequisites

Before you can start the HBAnyware Security Configurator, you must have the following items installed on your system:

- The SCSIport Miniport driver is properly installed.
- The HBAnyware and lputilnt utilities are properly installed.
- The HBAnyware Security Configurator is properly installed.

Note: Before you start the Configurator, you must make sure that all of the systems that are part of, or will be part of, the security configuration are online on the Fibre Channel network so that they receive updates or changes made to the security configuration. Any system that is already part of the security installation might not run with the proper security attributes, if updates to the security configuration are made while it is offline.
Any system that is part of the security installation and that is offline when the HBAnyware Security Configurator starts will not be available for security configuration changes even if it is brought online while the Configurator is running.

Procedure

To start the HBAnyware Security Configurator:

1. Run the /usr/sbin/hbanyware/ssc script. Type:

   ```
   /usr/sbin/hbanyware/ssc
   ```

Running the Security Configurator for the First Time/Create the ACG

When you install the HBAnyware Security software on a system and run the HBAnyware Security Configurator for the first time, that system becomes the Master Security Client (MSC). All of the available servers are discovered and are available to be part of the system Access Control Group (ACG). You select the systems to add to the ACG, and the security configuration updates on all of the selected servers as well as on the initial system. This selection constitutes the participating platforms in this security installation.

To create the ACG:

1. Start the Security Configurator for the first time in an unsecure environment. The following message appears:

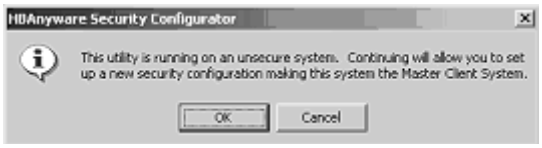
HBAnyware Security Configurator
This utility is running on an unsecure system. Continuing will allow you to set up a new security configuration making this system the Master Client System.
OK
Cancel

Figure 62: HBAnyware Security Configurator "Unsecure System" Message

2. Click **OK**. The Access Control Group tab appears:

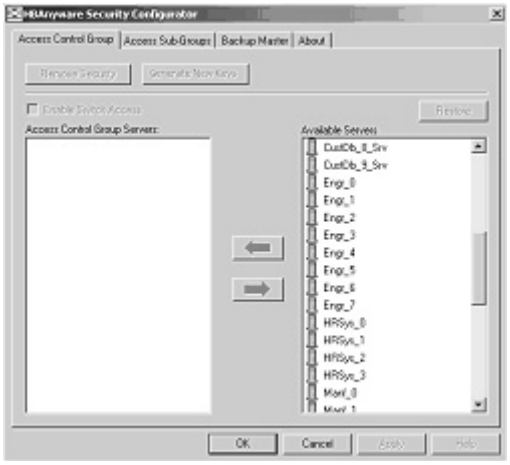

Figure 63: HBAnyware Security Configurator, Access Control Group Tab, No ACG Servers

3. Select the unsecured servers that you want to add to the ACG from the Available Servers list.

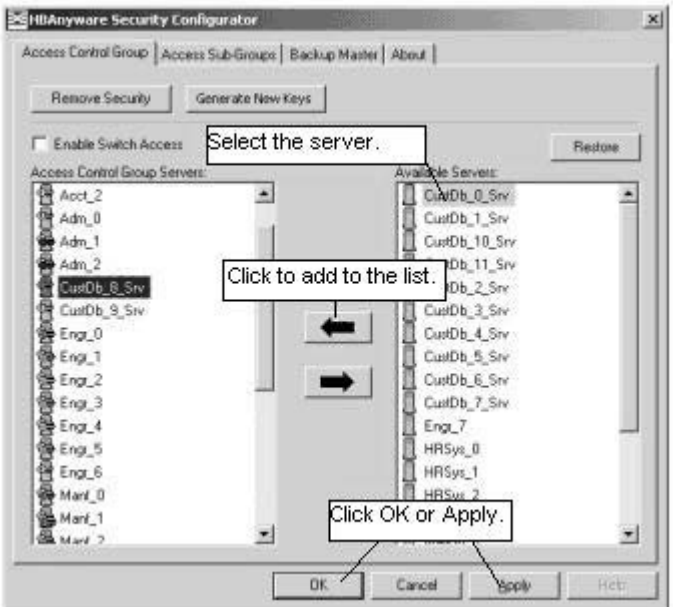

Figure 64: HBAnyware Security Configurator, Access Control Group Tab with ACG Servers

4. Click the **left arrow** to add the servers to the Access Control Group Servers list.
5. Click **OK** or **Apply**.

Designating a Master Security Client

The first time you run the Security Configurator on any system in a FC network, that system becomes the Master Security Client (MSC). See “Running the Configurator for the First Time” on page 120 for more information.

Setting Up and Maintaining Access Control Groups

Introduction

The Access Control Group tab shows the systems that are part of a client's Access Control Group (ACG) and, from the Master Security Client (MSC), allows you to select the systems that belong to the ACG.

Selecting/Deselecting Access Control Group Tab on the MSC

On the MSC, you select or deselect the systems that are to be part of the security installation in the Access Control Group tab. When you select unsecure systems and move them to the Access Control Group Servers list, these systems updates to secure them and bring them into the MSC's ACG. When you select systems in the ACG and move them to the Available Servers list, the security configuration for those systems update to make them unsecure. After you have configured security from the MSC for the

first time, the Access Control Group tab looks similar to the following:

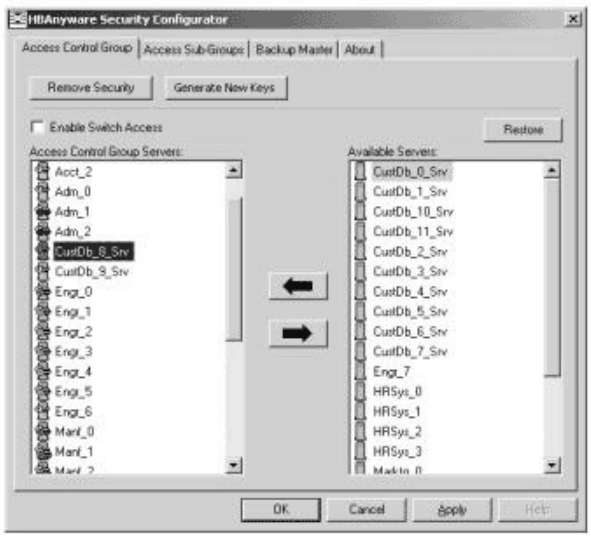

Figure 65: HBAnyware Security Configurator, Access Control Group Tab on an MSC System

Viewing the Access Control Group Tab on a Non-MSC

On a non-MSC system, the Access Control Group tab shows the systems that are part of the client's ACG. You cannot modify the ACG on a non-MSC. (You can modify the ACG only on the MSC or a client higher in the security topology's hierarchy.) The Access Control Group tab on a non-MSC system looks similar to the following:

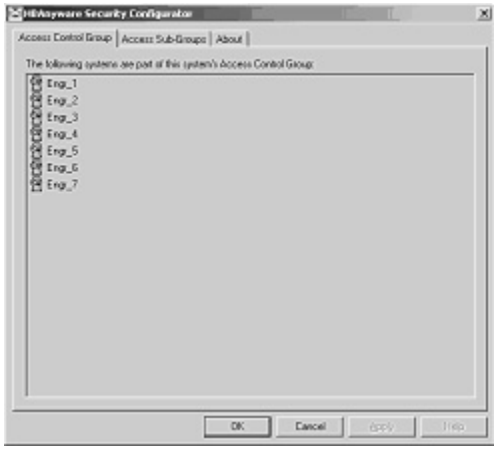

Figure 66: HBAnyware Security Configurator, Access Control Group Tab on a Non_MSC System

Table 13: Access Control Group-Specific Buttons

Button Title	Corresponding Procedure
Remove Security	Remove security from all servers in the ACG
Generate New Keys	Generate new security keys.
Restore	Restore the ACG to its last saved configuration.

ACG Icons

Depending on the configured security topology, a system can be a server in one or more ACGs. It can also be a client to an ACG. The following icons indicate the state of each of the systems in the Access Control Group Servers list.

The system is a secure server in the ACG. It does not belong to an Access Sub-Group (ASG). You can remove this system from the ACG.

The system is a secure server in the ACG and belongs to one or more ASGs. You can remove this system from the ACG.

The system is a secure server in the ACG and a client to an ASG. You cannot remove this system from the ACG until you remove it as a client from the ASG.

The system is a secure server in the ACG, a secure server in one or more ASGs and a client to an ASG. You cannot remove this system from the ACG until you remove it as a client from the ASGs.

The system is a Backup Master. You cannot remove this system from the ACG until you remove it as a Backup Master.

Running the Configurator for the First Time/Creating the ACG

When you install the HBAnyware Security software on a system and run the HBAnyware Security Configurator for the first time, that system becomes the Master Security Client (MSC). All of the available servers are discovered and available to become part of the system Access Control Group (ACG). Select the systems to add to the ACG, and the security configuration updates all of the selected servers as well as on the initial system. This selection constitutes the participating platforms in this security installation.

To create the ACG:

1. Start the HBAnyware Security Configurator for the first time in an unsecure environment. The computer from which you run the Configurator becomes the MSC. The “Unsecured System” message appears (see Figure 62).
2. Click **OK**. The Access Control Group tab appears (Figure 63).
3. Select the unsecured servers that you want to add to the ACG from the Available Servers list (Figure 65).
4. Click the **left arrow** to add the servers to the Access Control Group Servers list.
5. Click **OK** or **Apply**.

Adding a Server to the ACG

After you create the initial Access Control Group (ACG) on the Master Security Client (MSC), you may add unsecured servers to the ACG.

To add servers to the ACG:

1. Start the HBAnyware Security Configurator.
2. On the Access Control Group tab, from the Available Servers list, select the unsecured servers to add to the ACG (Figure 65).
3. Click the **left arrow** to add the server to the Access Control Group Servers list.
4. Click **OK** or **Apply**.

Deleting a Server from the ACG

To delete a server from the Access Control Group (ACG):

1. Start the HBAnyware Security Configurator.
2. On the Access Control Group tab, from the Access Control Group Servers list, select the secured systems to delete from the ACG (Figure 65).
3. Click the **right arrow** to remove the servers from the Access Control Group Servers list.
4. Click **OK** or **Apply**.

Removing Security from All Servers in the ACG

You can remove security from all systems only from the Master Security Client (MSC). Removing the entire security topology on all of the servers in the MSC's ACG puts the servers in an unsecure state. The MSC is also put in an unsecure state; consequently, it is no longer the MSC. Any participating systems that are not online will not receive the 'remove security' configuration update, and as a result will no longer be accessible remotely.

To remove security from all servers in the ACG:

1. Start the HBAnyware Security Configurator. The Access Control Group tab appears (Figure 65).
2. On the Access Control Group tab, click the **Remove Security** button. The following message appears:

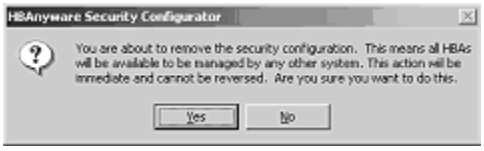
HBAnyware Security Configurator
You are about to remove the security configuration. This means all HBAs will be available to be managed by any other system. This action will be immediate and cannot be reversed. Are you sure you want to do this.
Yes
No

Figure 67: HBAnyware Security Configurator, "Warning" Dialog Box

3. Click **Yes**. Security is removed from all servers in the ACG.

Generating New Security Keys

You can generate new security keys only from a Master Security Client (MSC). After the new security keys are generated, they are automatically sent to all of the remote servers in the Access Control Group (ACG).

Note: All the servers that are part of the ACG must be online when this procedure is performed so that they may receive the new keys. Any servers that do not receive the new keys will no longer be accessible remotely.

To generate new security keys for all servers in the ACG:

1. From the MSC, start the HBAnyware Security Configurator. The Access Control Group tab appears (Figure 63 on page 120).
2. On the Access Control Group tab, click the **Generate New Keys** button. A dialog box warns you that you are about to generate new security keys for all systems.
3. Click **Yes**. The new keys generate and are sent to all of the remote servers in the ACG.

Restoring the ACG to Its Last Saved Configuration

You can restore the ACG to its last saved configuration, if there are unsaved changes to the ACG, only from the Master Security Client (MSC).

To restore the ACG to its last saved configuration:

1. From the Access Control Group tab on the MSC, click the **Restore** button (Figure 65).

Accessing a Switch

You can enable switch access only on a Master Security Client (MSC). Switch access grants the client access rights to a switch to remotely access HBAs on servers in the Access Control Group (ACG).

To enable switch access:

1. Start the HBAnyware Security Configurator.
2. From the Access Control Group tab, check Enable Switch Access. (Figure 65).

Setting Up and Maintaining Access Sub-Groups

Introduction

Use the Access Sub-Group tab to create multiple Access Sub-Groups (ASGs) and multiple levels (tiers) in the security topology hierarchy. The hierarchy can be as many levels deep as desired. However, we recommend the hierarchy extend no more than three levels deep, as it becomes increasingly difficult to keep track of the topology the deeper it goes. The hierarchy shows in the Access Sub-Groups tab as a tree. You can create, modify and delete ASGs at each level in this tree.

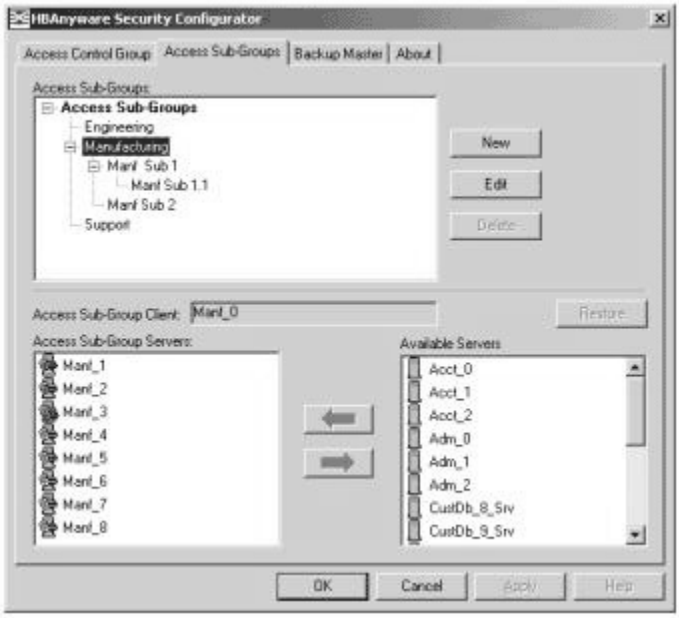

Figure 68: HBAnyware Security Configurator, Access Sub-Groups Tab with Sub-Groups Created

Table 14: Access Sub-Group-Specific Buttons

Button Title	Corresponding Procedure
New	Add a server to the ACG.
Edit	Generate new security keys.
Delete	Delete an ASG.
Restore	Restore the ACG to its last saved configuration.

ASG Icons

The following icons indicate the state of each of the servers in the Access Sub-Group Servers list.

The system is a server in the ASG but not in any child ASGs. You can remove it from the ASG.

The system is a server in the ASG and at least one child ASG. You cannot remove it from the ASG until you remove it from the child ASGs.

The system is a server in the ASG and a client to a child ASG. You cannot remove it from the ASG until you remove it as a client from the child ASG (by either deleting or editing the child ASG).

The system is a server in the ASG, a server in at least one other child ASG and a client to a child ASG. You cannot remove it from the ASG until you remove it from the child ASGs and as a client from the child ASG (by either deleting or editing the child ASG).

The system is a server in the ASG and a client to a non-child ASG. You can remove it from the ASG.

The system is a server in the ASG, a server in at least one child ASG, and a client to a non-child ASG. You cannot remove it from the ASG until you remove it from the child ASGs.

Creating an ASG

Create a new Access Sub-Group (ASG) by selecting one system from the Access Control Group (ACG) to be the client, and some or all of the other systems to be servers to this client, thus defining the new client's ACG. When the HBAnyware Security Configurator is run on the new client, the ACG shows the servers that were configured in the ASG by its parent client.

To create an ASG:

1. Start the HBAnyware Security Configurator.
1. Click the Access Sub-Groups tab.

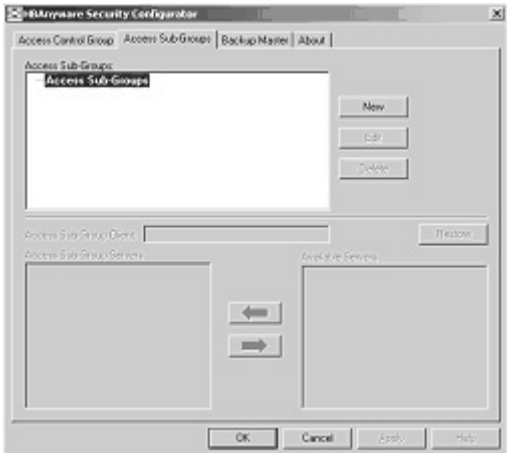

Figure 69: HBAnyware Security Configurator, Access Sub-Groups Tab with No Sub-Groups Created

2. Click **New**. The New Access Sub-Group dialog box appears:

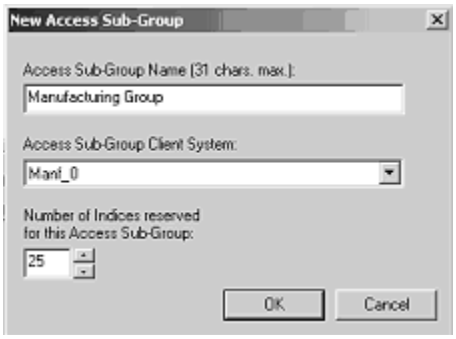

Figure 70: HBAnyware Security Configurator, New Access Sub-Group Dialog Box

3. Enter the ASG information:
    - Access Sub-Group Name: Enter the name of the ASG. The ASG name is for identification purposes only. It does not provide any security function. Provide a name that will make it easy to remember the systems that are part of the ASG. The name can contain any alphanumeric characters, symbols or spaces (up to 31). At each level of the security topology, each ASG name must be unique. If the name is not unique at its level, an error message informs you of this when you click **OK**.
    - Access Sub-Group Client System: Select the system that is to be the client.
    - Number of indices reserved for this Access Sub-Group: Select the number of 'indices' you want to reserve for the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that you can subsequently create on the new client's system.
4. Click **OK** in the New Access Sub-Group window. The ASG is created.

Reserved Indices - Examples

A particular security installation can support the creation of several hundred access groups (ACGs and ASGs). When you create each new access group, you allocate some number of 'indices' to the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that you can subsequently create at the new client's system.

- If zero indices are reserved, you cannot create any lower-level ASG under the client of the new ASG. Thus, for example, if you want to implement a multi-tiered security architecture consisting of many ASGs, and you want to create them all from the Master Security Client (MSC), zero indices would be allocated to each of the new ASGs client platforms when they are created.
- If you create an ASG, and you reserve 25 indices for the new ASG client platform, a child ASG created by this platform will have a maximum of only 24 indices available to be reserved (one is taken by the creation of the child ASG itself). This continues down the ASG hierarchy as each lower level ASG is created.
- When you create an ASG from the MSC, a maximum of 50 indices (or less if fewer are available) can be reserved. For all other clients, the maximum depends on how many indices were reserved to that client when its ASG was created, and on how many it has subsequently allocated to its ASGs.

Adding a Server to an ASG

To add a server to an ASG:

1. Start the HBAnyware Security Configurator.
2. Click the Access Sub-Group tab.
3. The name of the ASG is displayed in the Access Sub-Groups tree. From the Available Servers list, select the servers to be added to the ASG.

   Note: Out-of-band servers appear in the Available Servers list even though the ASG client system may not have discovered them yet. You can still add these servers to the Access Sub-Group Servers list.

4. Click the **left arrow** to move the servers to the Access Sub-Group Servers list.
5. Click **OK** or **Apply** to update servers, adding them to the ASG. The new client can remotely manage the HBAs on those servers using the HBAnyware utility.

Deleting an ASG

Only a leaf node ASG may be deleted (i.e. not ASGs underneath it in the tree). If an ASG has at least one child ASG, those child ASGs must be deleted first.

To delete an ASG:

1. Start the HBAnyware Security Configurator.
2. From the Access Sub-Group tree, select the leaf node ASG you wish to delete.
3. Press the **Delete** button. A window appears warning you that if you continue the access sub-group will be deleted.
4. Click **Yes**. This operation is immediate. There is no need to press the **OK** or **Apply** button.

Restoring an ASG to Its Last Saved Configuration

You can restore an Access Sub-Group (ASG) to its last saved configuration if there are unsaved changes to it.

To restore an ASG to its last saved configuration:

1. Start the HBAnyware Security Configurator.
2. Click the Access Sub-Group tab.
3. Select the ASG whose configuration you want to restore.
4. Click **Restore**.
5. Click **OK** or **Apply** to save your changes.

Editing an ASG

You can change the name, client system or reserved indices of an Access Sub-Group (ASG).

To edit an ASG:

1. Start the HBAnyware Security Configurator.
2. Click the Access Sub-Group tab.
3. Select the ASG you want to edit.

4. Click **Edit**. The Edit Access Sub-Group window is displayed.

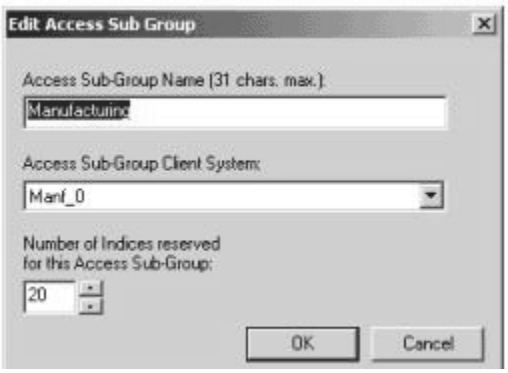

Figure 71: HBAnyware Security Configurator, Edit Access Sub Group Dialog Box

5. Change the ASG information:
    - Access Sub-Group Name: Change the name of the ASG. The ASG name is for identification purposes only. It does not provide any security function. Provide a name that is easy to remember the systems that are part of the ASG.
      The name can contain any alphanumeric characters, symbols or spaces (up to 31). At each level of the security topology, each ASG name must be unique. If the name is not unique at its level, an error message informs you of this when you click **OK**.
    - Access Sub-Group Client System: Select the new system to be the client. If the Configurator is running on a system connected to more than one fabric, the client list contains only those systems that can be accessed by the original client of the ASG.
    - Number of indices reserved for this Access Sub-Group: Select the new number of 'indices' to reserve for the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that you can subsequently create on the new client's system. See page 127 for examples.
6. Click **OK** in the Edit Access Sub-Group dialog box to save your changes.

About Offline ASGs

A client system may not be online when the HBAnyware Security Configurator is running. In this case, the Access Sub-Group (ASG) for the client appears offline in the ASG tree, much like the following:

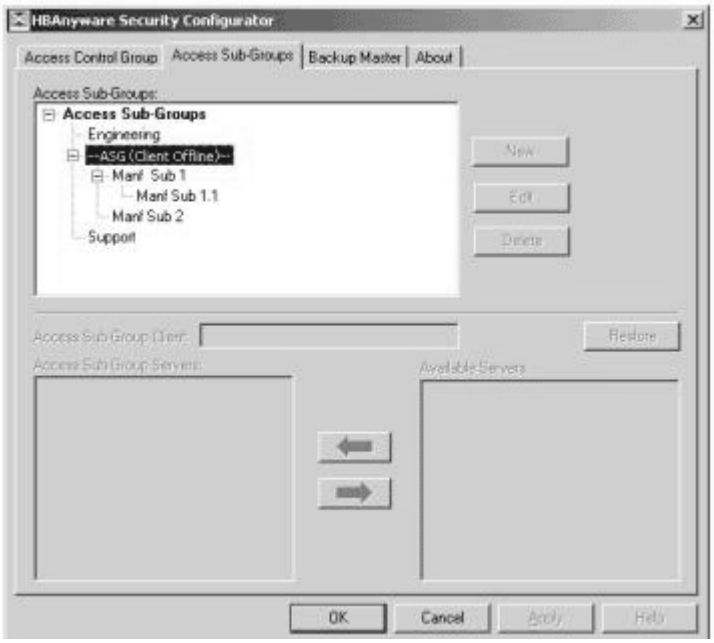

Figure 72: HBAnyware Security Configurator, Access Sub-Groups Tab - Client System Offline

The offline ASG entry serves as a placeholder for where the real ASG would be in the tree. You cannot modify or delete the entry (although it is removed from the display if all of its child ASGs are deleted).

It is possible to delete the child ASGs of an offline ASG. However, we recommend that you delete them only if the client for the offline ASG will never be put online again. It is best to delete child ASGs when the parent ASG is online.

If you choose to delete a child ASG, the operation is immediate. There is no need to click **OK** or **Apply**.

Backup Masters

Introduction

A Backup Master mirrors the security data of the Master Security Client (MSC) in case it has to take over as the MSC if the MSC is unable to operate or is removed from the security configuration. A Backup master system receives all the updates to the security configuration on the MSC. However, you cannot make modifications to the security configuration on a Backup Master.

When the Configurator runs on a Backup Master, the Access Control Group tab looks like the tab on a non-MSC system. The Access Sub-Group tab shows the ASGs, but you cannot change the ASGs (Figure 65 on page 122).

The Backup Master tab is available only when the HBAnyware Security Configurator is running on the MSC or a Backup Master. Use this tab to set up a system as a Backup Master to the MSC and to replace the MSC with a Backup Master.

Each time you start the HBAnyware Security Configurator on the MSC and no Backup Master is assigned, a message warns you that no Backup Master Client is assigned to the security configuration.

If you run the HBAnyware Security Configurator on a Backup Master, a message warns you that you can only view security information on a Backup Master. Security changes must be made to the MSC.

A Backup Master system receives all the updates that the MSC makes to the security configuration, therefore it is very important that the Backup Master is online when the HBAnyware Security Configurator is running on the MSC. Otherwise, updates to the security configuration are not reflected to the Backup Master. If the Backup Master then becomes the MSC, the security configuration may be corrupted.

Backup Master Eligible Systems

To be eligible to become a Backup Master, a system must not be a client or server in any ASG. In other words, it must be either a server in the MSC's Access Control Group (ACG) or an unsecure system. If it is an unsecure system, it will be secure when it becomes a Backup Master.

Backup Master Tab and Controls

The first time the Backup Master tab is selected on the MSC, it looks similar to Figure 73:

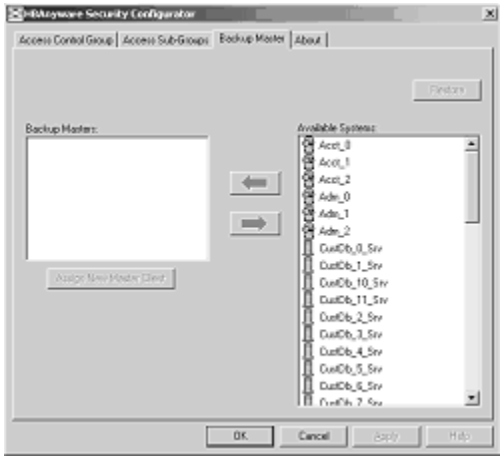

Figure 73: HBAnyware Security Configurator, Backup Master tab - First Time Selected

The following tasks are performed on the Backup Master tab.

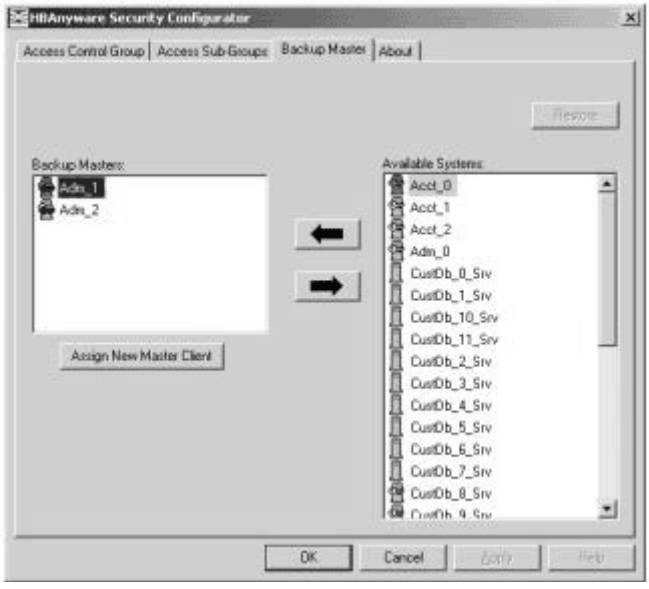

Figure 74: Backup Master Tab with Backup Masters Created

Table 6. Backup Master-Specific Buttons

Button Title	Corresponding Procedure
Assign This System As The Master Client	Reassign a Backup Master as the new MSC from the old MSC.
Edit	Generate new security keys.
Delete	Delete a Backup Master.
Restore	Restore the Backup Master to its last saved configuration.

Creating a Backup Master

To create a Backup Master:

1. On the MSC, start the HBAnyware Security Configurator.
2. Click the Backup Master tab.

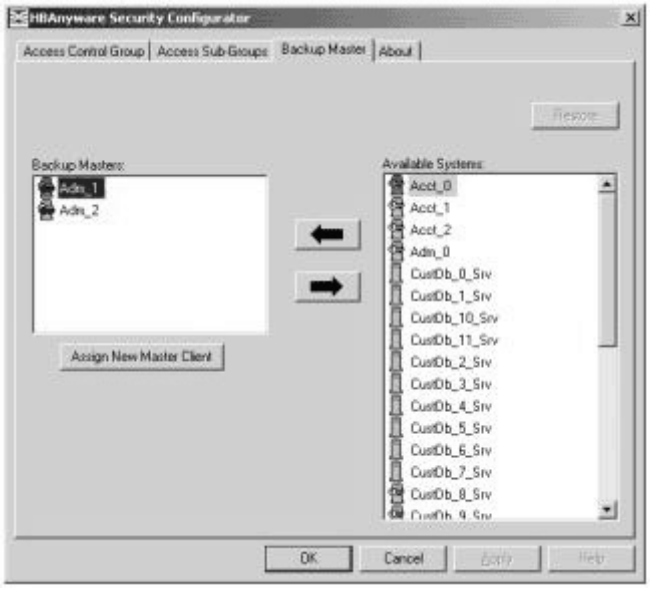

Figure 75: HBAnyware Security Configurator, Backup Master Tab with Backup Masters

3. Select a system from the Available Systems list.
4. Click the **left arrow** to move the system to the Backup Masters list.
5. Click **OK** or **Apply** to save your changes.

Reassigning a Backup Master as the New MSC from the Old MSC

Because a Backup Master may have to take over as the Master Security Client (MSC), it should be able to physically access all of the HBAs that the MSC can access. If the MSC connects to multiple fabrics, select its Backup Master from the Available Systems list connected to the same fabrics as the MSC.

To reassign a Backup Master as the new MSC from the old MSC:

1. On the MSC, start the HBAnyware Security Configurator.
2. Click the Backup Master tab.

3. In the Backup Masters list, select the Backup Master system to reassign as the MSC.
4. Click **Assign New Master Client**. You will be asked if you wish to proceed.
5. Click **Yes**. The selected Backup Master becomes the new MSC. The current MSC becomes a server in the new MSC's ACG. After the changes are made, a message indicates that the reassignment is complete.
6. Click **OK**. The Security Configurator closes because the system is no longer the MSC.

Reassigning the New MSC from the Backup Master

WARNING: Use this method only if the MSC cannot relinquish control to a Backup Master. For example, if the MSC is no longer bootable or able to connect to the FC network. Under any other circumstances, if the Backup Master takes over as the MSC, and the MSC is still running or comes back online later, there will be two MSCs for the same security configuration. This will eventually lead to corruption of the security configuration.

To reassign the new MSC from the Backup Master:

1. On the Backup Master system that you want to reassign as the MSC, start the Security Configurator.
2. Click the Backup Master tab. The following warning and button appear:

Figure 76: HBAnyware Security Configurator, Backup Master "Warning" Dialog Box

3. Click **Assign This System As The Master Client**. A prompt asks if you want to continue.
4. Click **Yes**. A prompt notifies you that this system is now the new MSC.
5. Click **OK**. The Configurator closes.
6. Restart the Security Configurator to run the former Backup Master as the MSC.

Troubleshooting

Introduction

There are several circumstances in which your system may operate in an unexpected manner. The Troubleshooting section contains reference tables on event codes and error messages and provides information regarding unusual situations.

Event Tracing (Windows Server 2003, SP1 only)

Trace messages are part of the Emulex lpfc log messages.

Storage Event Tracing supports two types of events:

- FFInit (0x00000001) - events that occurred at HwFindAdapter and HwInitialize.
- FFIo (0x00000002) - events that occurred during I/O.

Storage Event Tracing supports four levels of events:

- DbgLvlErr (0x00000001) - error level
- DbGLvlWrn (0x00000002) - warning level
- DbgLvlInfo (0x00000004) - Information level
- DbgLvlInfo (0x00000008) - excessive information level

Note: To view trace messages, you must enable Event Tracing in the operating system. See your Microsoft operating system documentation for more information.

Event Trace Messages

ELS Log Messages (0101 - 0117)

lpfc_mes0101: “0101: FLOGI completes successfully - IoTag <ioTag x%x>, Word4 <ulpWord[4]x%x>, e_d_tov <EdTov x%x)>, r_a_tov <RaTov x%x>, edtov resolution <EdTovResolution x%x>”

DESCRIPTION: An ELS FLOGI command that was sent to the fabric succeeded.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.
SEE ALSO: lpfc_mes0110.

lpfc_mes0102: “0102: PLOGI completes to NPort DID <did %06x> - IoTag <ioTag x%x>, Status <cmdStatus x%x>, Word4 <ulpWord[4] x%x>”

DESCRIPTION: The HBA performed a PLOGI into a remote NPort.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.
SEE ALSO: lpfc_mes0110.

lpfc_mes0103: “0103:PRLI completes to NPort DID <did %06x> - IoTag <ioTag x%x>, Status <cmdStatus x%x>, Word4 <ulpWord[4] x%x> PRLIsp Word3 <FC Parm Word 3 x%x>”

DESCRIPTION: The HBA performed a PRLI into a remote NPort. PRLIRsp Word 3 is only shown if the PRLI response is valid.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.
SEE ALSO: lpfc_mes0110.

lpfc_mes0104: “0104: ADISC completes to NPort DID <did %06x> - IoTag <ioTag x%x>, Status <cmdStatus x%x>, Word4 <ulpWord[4] x%x>"

DESCRIPTION: The HBA performed an ADISC into a remote NPort.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.
SEE ALSO: lpfc_mes0110.

lpfc_mes0110: “0110: ELS response - ElsCmd <elsCmd x%x>, IoTag <ioTag x%x>, Status <cmdStatus x%x>, Word4 <ulpWord[4] x%x>”

DESCRIPTION: The specific ELS response was completed by the firmware.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.
REMARKS: lpfc_mes0101, lpfc_mes0102, lpfc_mes0103 or lpfc_mes0104 are also recorded for more details. You can use the IOTag to match the messages.
SEE ALSO: lpfc_mes0116

lpfc_mes0112: “0112: ELS command <elsCmd x%x> received from NPORT DID <did %06x>, XRI <xri x%x> - State <hbaState x%x>”

DESCRIPTION: Received the specific ELS command from a remote NPort.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.
REMARKS: lpfc_mes0113, lpfc_mes0114, lpfc_mes0115 or lpfc_mes0117 are also recorded for more details if the corresponding SEVERITY level is set. You can use the XRI to match the messages.

lpfc_mes0113: “0113: An FLOGI ELS command <elsCmd x%x> was received from DID <did %06x> XRI <xri x%x> in Loop Mode"

DESCRIPTION: While in Loop Mode an unknown or unsupported ELS command was received.
SEVERITY: Error
LOG: LOG_ELS verbose
ACTION: Check device DID
SEE ALSO: lpfc_mes0112.

lpfc_mes0114: "0114: PLOGI chkparm OK - XRI <xri x%x>, DID <did %06x>, WWPN <wwpn %08x%08x>, Flags <NodeFlags x%x>, State <NodeState x%x>, RPI <rpi x%x>"

DESCRIPTION: Received a PLOGI from a remote NPORT and its Fibre Channel service parameters match this HBA. Request can be accepted.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.
SEE ALSO: lpfc_mes0112.

lpfc_mes0115: "0115: Unknown ELS command <elsCmd x%x> received from NPORT, DID <did %06x> XRI <xri x%x>"

DESCRIPTION: Received an unsupported ELS command from a remote NPORT.
SEVERITY: Error
LOG: LOG_ELS verbose
ACTION: Check remote NPORT for potential problem.
SEE ALSO: lpfc_mes0112.

lpfc_mes0116: "0116: Xmit ELS command <elsCmd x%x> to remote NPORT DID <did %06x> - IoTag <ioTag x%x>, State <hbaState x%x>"

DESCRIPTION: Xmit ELS command to remote NPORT.
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational
remark: lpfc_mes 110 is recorded for the response of the ElsCmd. The IoTag can be used to match lpfc_mes0116 and lpfc_mes0110.
SEE ALSO: lpfc-mes0714.

lpfc_mes0117: "0117: Xmit ELS response <rspCode x%x> for ELS Command <elsCmd x%x> to remote NPORT XRI <xri x%x>”

DESCRIPTION: Xmit ELS response to remote NPORT
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational
SEE ALSO: lpfc_mes 0112.

Discovery Log Messages (0201 - 0246)

lpfc_mes0201: "0201: Abort outstanding I/O on NPort DID <DID %06x> WWPN <wwpn %08x%08x> - Flags <NodeFlags x%x>, State <NodeState x%x>, RPI <rpi x%x>"

DESCRIPTION: All outstanding I/Os are cleaned up on the specified remote NPort.
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational

lpfc_mes0202: "0202: Start Discovery state <hbaState x%x> - TMO <tmo %d>, DISC CNT <discCnt %d>, RSCN CNT <RscnCnt %d>"

DESCRIPTION: Device discovery/rediscovery after FLOGI, FAN or RSCN has started. TMO is the current value of the soft link time. It is used for link discovery against the linkDownTime set in parameters. DISC CNT is number of nodes being discovered for link discovery. RSCN CNT is number of nodes being discovered for RSCN discovery. So, there will be value in either DISC CNT or RSCN CNT depending which discovery is being performed.
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

lpfc_mes0203: "0203: Nodev timeout on NPort DID <DID %06x> WWPN <wwpn %08x%08x> - Flags <NodeFlags x%x>, State <NodeState x%x>, RPI <rpi x%x>"

DESCRIPTION: A remote NPort that was discovered by the driver disappeared for more than ELX_NODE_TMO seconds.
SEVERITY: Error
LOG: LOG_DISCOVERY verbose
ACTION: Check connections to Fabric / HUB or remote device.

lpfc_mes0224: "0224: NameServer Query timeout - R_A_TOV <ratov x%x>, Retry Cnt, <retryCnt %d> Max Retry <maxRetryCnt %d>"

DESCRIPTION: Node authentication timeout, node Discovery timeout. A NameServer Query to the Fabric or discovery of reported remote NPorts is not acknowledged within 3*R_A_TOV.
SEVERITY: Error
LOG: LOG_DISCOVERY verbose
ACTION: Check Fabric configuration. The driver recovers from this and continues with device discovery.

lpfc_mes0225: "0225: Device Discovery completes"

DESCRIPTION: This indicates successful completion of device (re)discovery after a link up.
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

lpfc_mes0229: "0229: Assign scsi Path (path %d> Target <%d> to NPort DID <DID %06x> WWPN <wwpn %08x%08x> - BindType <bindType x%x>, Flags <NodeFlags x%x>, State <NodeState x%x>, RPI <rpi x%x>"

DESCRIPTION: The driver assigned a SCSI ID to a discovered mapped FCP target. BindType - 0: DID 1:WWNN 2:WWPN
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

lpfc_mes0236: "0236: NameServer Req - Command <cmdCode x%x>, State <hbaState x%x>, RSCN CNT <rscnCnt %d>"

DESCRIPTION: The driver is issuing a nameserver request to the fabric. Also recorded if a GID_FT is sent.
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.
SEE ALSO: lpfc_mes0239 or lpfc_mes0240.

lpfc_mes0239: "0239: NameServer Rsp - DID <DID %06x>, State <hbaState x%x>, RSCN CNT <rscnCnt %d"

DESCRIPTION: The driver received a nameserver response. And, this message is recorded for each DID included in the response data.
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

SEE ALSO: lpfc_mes0236.

"lpfc_mes0240: "0240: NameServer Rsp Error - Command Rsp <Command-Response.bit.CmdRsp x%x>, Reason Code <ReasonCode x%x>, Explanation <explanation x%x>, State <hbaState x%x>"

DESCRIPTION: The driver received a nameserver response containing a status error.
SEVERITY: Error
LOG: LOG_DISCOVERY verbose
ACTION: Check Fabric configuration. The driver recovers from this and continues with device discovery.
SEE ALSO: lpfc_mes0236.

lpfc_mes0246: "0246: RegLogin failed - Did <Did %06x>, Mailbox Status <mbxStatus x%x> state <hbaState x%x>"

DESCRIPTION: Firmware returned failure for the specified RegLogin.
SEVERITY: Error
LOG: LOG_DISCOVERY verbose

ACTION: This message indicates that the firmware could not do. RegLogin for the specified Did. It could be because there is a limitation on how many nodes an HBA can see.

Mailbox Log Messages (0310 - 0326)

lpfc_mes0310: "0310: Mailbox command <cmd x%x> timeout - state <hbaState x%x>, sync <sync %d>"

DESCRIPTION: A Mailbox command was posted to the adapter and did not complete within 30 seconds. sync - 0: asynchronous mailbox command is issued 1: synchronous mailbox command is issued.
SEVERITY: Error
LOG: LOG_MBOX verbose
ACTION: This error could indicate a software driver or firmware problem. If no I/O is going through the adapter, reboot the system. If these problems persist, report these errors to Technical Support.

lpfc_mes0321: "0321: Unknown IOCB command - Command <cmdCode x%x>, Status <cmdStatus x%x>, IoTag <ulpIoTag x%x>, Context <ulpContext x%x>"

DESCRIPTION: Received an unknown IOCB command completion.
SEVERITY: Error
LOG: LOG_MBOX verbose
ACTION: This error could indicate a software driver or firmware problem. If these problems persist, report these errors to Technical Support.

lpfc_mes0326: "0326: Reset HBA - State <hbaState x%x>, EmulexOption <x%x>"

DESCRIPTION: The HBA has been reset.
SEVERITY: Information
LOG: LOG_MBOX verbose
ACTION: No action needed, informational.

INIT Log Messages (0413 - 0460)

lpfc_mes0413: "0413: Configuration parameter <parameter name %x> out of range [<minimum %d>, <maximum %d>] resetting to default value<default %d>"

DESCRIPTION: User is attempting to set a configuration parameter to a value not supported by the driver. Resetting the configuration parameter to the default value.
SEVERITY: Error config
LOG: LOG_INIT verbose
ACTION: Make necessary changes to lpfc configuration file.

lpfc_mes0436: "0436: Adapter failed to init, timeout, status reg <status x%x>"

DESCRIPTION: The adapter failed during powerup diagnostics after it was reset.
SEVERITY: Error
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. If problems persist report these errors to Technical Support.

lpfc_mes0440: "0440: Adapter failed to init, mbxCmd <cmd x%x> READ_REV detected outdated firmware <firmware version %c.%c%c%c%c%c>"

DESCRIPTION: Outdated firmware was detected during initialization.
SEVERITY: Error
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. Update firmware. If problems persist report these errors to Technical Support.

lpfc_mes0442: 0442: Adapter failed to init, mbxCmd <cmd x%x> CONFIG_PORT, mbxStatus <status x%x>"

DESCRIPTION: Adapter initialization failed when issuing CONFIG_PORT mailbox command.
SEVERITY: Error
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. If problems persist report these errors to Technical Support.

lpfc_mes0446: "0446: Adapter failed to init, mbxCmd <cmd x%x> CFG_RING, mbxStatus <status x%x>, ring <ring number %d>

DESCRIPTION: Adapter initialization failed when issuing CFG_RING mailbox command.
SEVERITY: Error
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. If problems persist report these errors to Technical Support.

lpfc_mes0447: "0447: Adapter failed init, mbxCmd <cmd x%x> CONFIG_LINK mbxStatus <status x%x>

DESCRIPTION: Adapter initialization failed when issuing CONFIG_LINK mailbox command.
SEVERITY: Error
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. If problems persist report these errors to Technical Support.

lpfc_mes0454: "0454: Adapter failed to init, mbxCmd <cmd x%x> INIT_LINK, mbxStatus <status x%x>"

DESCRIPTION: Adapter initialization failed when issuing INIT_LINK mailbox command.
SEVERITY: Error
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. If problems persist report these errors to Technical Support.

lpfc_mes0457: "0457: Adapter Hardware Error - Host Status Reg <status reg x%x>, SLIM A8 <a8 x%x>, SLIM AC <ac x%x>"

DESCRIPTION: The driver received an interrupt indicting a possible hardware problem.
SEVERITY: Error
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. If problems persist report these errors to Technical Support.

lpfc_mes0458: "0458: Bring Adapter online"

DESCRIPTION: The FC driver has received a request to bring the adapter online. This may occur when running HBAnyware.
SEVERITY: Warning
LOG: LOG_INIT verbose
ACTION: None required.

lpfc_mes0460: "0460: Bring Adapter offline"

DESCRIPTION: The FC driver has received a request to bring the adapter offline. This may occur when running HBAnyware.
SEVERITY: Warning
LOG: LOG_INIT verbose
ACTION: None required.

FCP Log Messages (0700 - 0737)

lpfc_mes0700: "0700: Start nodev timer Scsi Path <path %d> Target <target %d> - DID <DID %06x>, WWPN <wwpn %08x%08x>, Flags <NodeFlags x%x>, State <NodeState x%x>"

DESCRIPTION: A target disappeared from the Fibre Channel network. If the target does not return within nodev-tmo timeout, all I/O to the target will fail.
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: None required.

lpfc_mes0702: "0702: Issue Target Reset to TGT Scsi Path <path %d> Target <target %d> - DID <DID %06x>, WWPN <wwpn %08x%08x>, Flags <NodeFlags x%x>, State <NodeState x%x>, RPI <rpi x%x>"

DESCRIPTION: The SCSI layer detected that it needs to abort all I/O to a specific target. This results in an FCP Task Management command to abort the I/O in progress.
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: Check state of target in question.
SEE ALSO: lpfc_mes0713 and lpfc_mes0714.

lpfc_mes0713: "0713: SCSI layer issued Target Reset - Path <path %d>, Target <target %d>, DID <did %06x>, WWPN <wwpn %08x%08x>"

DESCRIPTION: The SCSI layer is requesting the driver to abort I/O to a specific target.
SEVERITY: Error
LOG: LOG_FCP verbose
ACTION: Check state of target in question.
REMARKS: lpfc_mes0702 is recorded for more details if the corresponding SEVERITY level is set.

lpfc_mes0714: "0714: SCSI layer issued Bus Reset - Path <path %d>"

DESCRIPTION: The SCSI layer is requesting the driver to abort all I/Os to all targets on this HBA.
SEVERITY: Error
LOG: LOG_FCP verbose
ACTION: Check state of targets in question.
REMARKS: If resetTPRLO=0 - a lpfc_mes0702 is recorded if the corresponding SEVERITY level is set. Otherwise, a lpfc_mes0116 is recorded that a TPRLO is sent if the corresponding mode and SEVERITY level is set.

lpfc_mes0716: "0716: FCP Read Underrun, expected <DataTransferLength x%x>, residual <resid x%x> - fcpi_parm <fcpi_parm x%x>, Cdb[0] <cdb0 x%x>"

DESCRIPTION: FCP device provided less data than was requested.
SEVERITY: Supplement Information
LOG: LOG_FCP verbose
ACTION: No action needed, informational.
SEE ALSO: lpfc_mes0730.

lpfc_mes0729: “0729: FCP cmd <cmnd> failed - Path <path %d>, Target <target %d>, Lun <lun %d>, Srb Status <SrbStatus x%x>, IOCB status <cmdStatus x%x>, Word4 <ulpWord[4] x%x>, Word7 <ulpWord[7] x%x>"

DESCRIPTION: The specified device failed an I/O FCP command.
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: Check the state of the target in question.
REMARKS: lpfc_mes0730 is also recorded if it is a FCP Rsp error.

lpfc_mes0730:"0730: FCP command failed - Flags <status2 x%x>, SCSI status <status3 x%x>, Residual <ResId x%x>, Sense len <SnsLen x%x>, Resp len <RspLen x%x>, Resp Code <RspCode x%x>"

DESCRIPTION: The FCP command failed with a response error.
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: Check the state of the target in question.
remark: lpfc_mes0716, lpfc_mes0734, lpfc_mes0736 or lpfc_mes0737 is also recorded for more details if the corresponding SEVERITY level is set.
SEE ALSO: lpfc_mes0729.

lpfc_mes0734: "0734: FCP Read Check Error - Req len <DataTransferLength x%x>,Residual <resid x%x>, fcpi_parm <fcpi_parm x%x>, Cdb[0] <cdb0 x%x>"

DESCRIPTION: The issued FCP command returned a Read Check Error.
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: Check the state of the target in question.
SEE ALSO: lpfc_mes0730.

lpfc_mes0736: "0736: Received Queue Full status from FCP device - Path <path %d>,Target <target %d>, Lun <lun %d>, Current <currentOutstanding %d>, Max <maxOutstanding x%x>"

DESCRIPTION: Received a Queue Full error status from specified FCP device.
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: No action needed, informational
SEE ALSO: lpfc_mes0730.

lpfc_mes0737: "0737: Check condition received - Srb Status <srbStatus x%x>,Scsi Status <status3 x%x>, Sense Key <SenseKey x%x>, ASC <asc x%x>, ASCQ <ascq x%x>"

DESCRIPTION: The issued FCP command resulted in a Check Condition.
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: No action needed, informational
SEE ALSO: lpfc_mes0730.

Node Log Message (0900)

lpfc_mes0900:"0900: Cleanup node for NPort DID <did %06x> WWPN <wwpn %08x%08x> - Flags <NodeFlags x%x>, State <NodeState x%x>, RPI <rpi x%x>"

DESCRIPTION: The driver node table entry for a remote NPort was removed.
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: No action needed, informational.

Link Log Messages (1301 - 1307)

lpfc_mes1301: "1301: Re-establishing Link - Host Status Reg <status reg x%x>, SLIM A8 <a8 x%x>, SLIM AC <ac x%x>"

DESCRIPTION: The driver detected a condition where it had to re-initialize the link.
SEVERITY: Information
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check physical connections to Fibre Channel network.

lpfc_mes1302: "1302: Invalid speed for the board: Reset link speed to auto: <LinkSpeed setting x%x>"

DESCRIPTION: The driver is re-initializing the link speed to auto-detect.
SEVERITY: Warning
LOG: LOG_LINK_EVENT verbose
ACTION: None required.

lpfc_mes1303: "1303: Link Up Event <eventTag x%x> received - Last Event <fc_eventTag x%x>, Topology <Topology x%x>, Link Speed <LinkSpeed %d> (SpeedFlag <RdLA speedFlag x%x>), ALPA <granted_AL_PA x%x>, Map Entries <alpa_map[0] %d>

DESCRIPTION: A link up event was received. It is also possible for multiple link events to be received together.
SEVERITY: Error
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check physical connections to Fibre Channel network.
REMARKS: lpfc_mes1304 is recorded if Map Entries > 0 and corresponding mode and SEVERITY level is set.

lpfc_mes1304: "1304: Link Up Event ALPA map - <wd1 x%x> <wd2 x%x> <wd3 x%x> <wd4 x%x>"

DESCRIPTION: A link up event was received and an ALPA map was also received. Each message contains up to 16 ALPAS. Map Entries of lpfc_mes1303 should be used to determine the valid ALPAs.
SEVERITY: Warning
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check physical connections to Fibre Channel network.
SEE ALSO: lpfc_mes1303.

lpfc_mes1305:"1305: Link Down Event <eventTag x%x> received - Last Event <fc_eventTag x%x>, state <hbaState x%x>"

DESCRIPTION: A link down event was received.
SEVERITY: Error
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check physical connections to Fibre Channel network.

lpfc_mes1306: "1306: Link Down timeout - state <hbaState x%x>, Current TOV, <HLinkTimeOut %d>"

DESCRIPTION: The link was down for greater than the configuration parameter (HLinkTimeOut) seconds. All I/O associated with the devices on this link will be failed.
SEVERITY: Warning
LOG: LOG_LINK_EVENT verbose
ACTION: Check HBA cable/connection to Fibre Channel network.

lpfc_mes1307:1307: READ_LA mbox error <mbxStatus x%x> state <hbaState x%x>"

DESCRIPTION: The driver cannot determine what type of link event occurred.
SEVERITY: Information
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check physical connections to Fibre Channel network. Could indicate possible hardware or firmware problem.

Error Log

Viewing the Error Log

To view the error LOG:

1. Open the **E**vent Viewer window:
   - Click Start, Programs, Administrative Tools and Event Viewer

     or
   - Right-click on My Computer, select Manage and click on Event Viewer in Computer Management.

   The Event Viewer window is displayed.
2. Double-click any event with the source nameLPxNDS
3. Examine the entry at offset 0x10 and Event ID 11.

Note: Event ID 9's are not logged by the Emulex® SCSIport Miniport driver. These messages can be decoded using MS Q Article Q182335.

The Fibre Channel (FC) SCSIport Miniport driver logs events and errors in the operating system event log. Serious errors are always logged, while informational events are logged only if the parameter “LogErrors=1” is used. All logged events are issued an event ID of 11, Internal Adapter Error, but this does not necessarily indicate that an adapter error occurred. There are several exceptions:

0xC1 is logged as BAD FIRMWARE WARNING (event ID 26)

0xC2 is logged as BAD FIRMWARE WARNING (event ID 26)

0xED is logged as BUS TIMEOUT (event ID 9)

Event Log Tables

Byte offset 0x10 of the event is the driver event code, while byte offset 0x11-0x13 contains event-specific information.

Entries marked with an asterisk (*) are logged only when “LogErrors=1” is used.

Table 15: Error Log Table

0x10	Offset Explanation	0x11-0x13 further information
0xC0	Invalid Link Speed Selection	
0xC1	AutoTopology not supported in this firmware	Current firmware version 0x11 bit 4-7: major rev 0x11 bit 0-3 0x12 bit 4-7: minor rev 0x12 bit 0-3: 1=A, 2=B, 3=N, 4=X 0x13 bit 0-7: patch level e.g. 0x11 = 0x30 0x12 = 0x24 0x13 = 0x02 ==> 3.02x2
0xC2	Invalid data fix is not supported in this firmware	Current firmware version (see 0xC1)
0xC3*	Reestablishing Link	
0xD0	SNS_REQ (XMIT_SEQ) failed	0x11= cmdStat, 12= Parm err
0xD1	SNS_RSP (RCV_SEQ) failed	0x11= cmdStat, 12= Parm err
0xD2	No Resources	0x11= 0: Iocb cmd 1: Mailbox cmd, 0x12= cmd
0xD3*	RCV_ELS_REQ failed	0x11= cmdStat, 12= Parm err
0xD4*	XMT_ELS_REQ failed	0x11= cmdStat, 12= Parm err
0xD5	Too many targets found (160+)	0x11 - 13 = D_ID that didn't fit
0xD6*	SNS request timeout	0x11 - 13 no additional information
0xD7*	Mailbox interrupt timeout	0x11 = mailbox word 0
0xD8*	TPRLO requested when busy	0x11 = local req. state, 12= discState, 13= mailbox word 0
0xD9*	Link down timeout occurred	0x11 = local req. state, 12= discState, 13= mailbox word 0
0xDA*	Hard link down timeout occurred	0x11 = local req. state, 12= discState, 13= mailbox word 0
0xE0*	Node purged from configuration	0x11 - 0x13 = D_ID of node purged
0xE1	Error interrupt occurred	Status register bytes 1-3 in event 11-13. E1 error indicates an adapter hardware failure, return this host adapter for repair
0xE2	Mailbox cmd timeout	0x11= command
0xE3	Mailbox rsp err	0x11= command, 12-13 = mbxStatus
0xE4	Adapter not ready after initialization	Status register bytes 1-3 in event 11-13
0xE6	Mailbox int but cmd not complete	0x11= MB cmd, 12-13 = mbxStatus
0xE7	SRB already queued to ring	

Table 15: Error Log Table (Continued)

0x10	Offset Explanation	0x11-0x13 further information
0xE8	Restart failed	
0xE9	Port bypass (LPB) received	
0xEB	Unknown IOCB cmd rsp	0x11= 15:8=cmd field
0xEC	Uncached extension alloc. error	
0xED	Link down @boot time (30 sec.)	
0xEF	Too many interrupts at initial boot	
0xF0*	Rcv ELS Request (possible logout)	0x11= ELS type, 12-13 = X_ID
0xF1	LinkUp error; LP6/7 down, driver up	0x11= parameter field, 12=IOCB cmd
0xF2	LinkUp with illegal or corrupt RPI	0x11= parameter field, 12=IOCB cmd
0xF3*	DeQueue ring->iotCmd.head	0x11= caller ID
0xF4	Adapter reset	0x11 = coded reason for reset: bit 0 = IOCB Requeue; bit 1=ReadLa retry bit 2 = InitLink retry; bit 3=RstBus retry bit 4 = mailbox time out
0xF5*	FCP_IXXX_CR IOCB rsp err	0x11= cmdStat, 12= Parm err, 13= AL_PA
0xF6*	FCP_IXXX_CX IOCB rsp err	0x11= cmdStat, 12= Parm err, 13= AL_PA
0xF8	Invalid FCP_RSP	0x11 = FcpCntrl, 12 = ScsiStat, 13 = Len
0xFA	START_IO error	0x11 = ErrType, 12 = SrbStat, 13 = LinkUp
0xFB*	ELS_REQ_CR IOCB rsp err	0x11= cmdStat, 12= Parm err, 1 3= AL_PA
0xFC*	ELS_REQ_CX IOCB rsp err	0x11= cmdStat, 12= Parm err, 13 = AL_PA
0xFE*	FLOGI failed	0x11= cmdStat, 12= Parm err

Table 16: CmdStat Values

CmdStat	Value	Description
IOSTAT_FCP_RSP_ERR	0x1	
IOSTAT_REMOTE_STOP	0x2	Remote sent an ABTS
IOSTAT_LOCAL_REJECT	0x3	Parameter field contains additional info
IOSTAT_NPORT_RJT	0x4	
IOSTAT_FABRIC_RJT	0x5	
IOSTAT_NPORT_BSY	0x6	
IOSTAT_FABRIC_BSY	0x7	
IOSTAT_INTERMED_RSP	0x8	
IOSTAT_LS_RJT	0x9	Remote sent LS_RJT
IOSTAT_BA_RJT	0xA	Remote sent BA_RJT

Table 17: Parameter Error Values (valid only when CmdStat value = 0x3)

Parameter Error	Value	Description
IOERR_SUCCESS	0x00	
IOERR_MISSING_CONTINUE	0x01	
IOERR_SEQUENCE_TIMEOUT	0x02	Possible bad cable/link noise
IOERR_INTERNAL_ERROR	0x03	
IOERR_INVALID_RPI	0x04	Remote port login data invalid
IOERR_NO_XRI	0x05	
IOERR_ILLEGAL_COMMAND	0x06	
IOERR_XCHG_DROPPED	0x07	
IOERR_ILLEGAL_FIELD	0x08	
IOERR_BAD_CONTINUE	0x09	
IOERR_TOO_MANY_BUFFERS	0x0A	
IOERR_RCV_BUFFER_WAITING	0x0B	
IOERR_NO_CONNECTION	0x0C	
IOERR_TX_DMA_FAILED	0x0D	
IOERR_RX_DMA_FAILED	0x0E	
IOERR_ILLEGAL_FRAME	0x0F	Possible bad cable/link noise
IOERR_EXTRA_DATA	0x10	
IOERR_NO_RESOURCES	0x11	
IOERR_RESERVED	0x12	
IOERR_ILLEGAL_LENGTH	0x13	
IOERR_UNSUPPORTED_FEATURE	0x14	
IOERR_ABORT_IN_PROGRESS	0x15	

Table 17: Parameter Error Values (valid only when CmdStat value = 0x3) (Continued)

Parameter Error	Value	Description
IOERR_ABORT_REQUESTED	0x16	
OERR_RECEIVE_BUFFER_TIMEOUT	0x17	
IOERR_LOOP_OPEN_FAILURE	0x18	FC_AL target not responding. Received our own transmitted frame back. Port may be bypassed by a hub
IOERR_RING_RESET	0x19	
IOERR_LINK_DOWN	0x1A	
IOERR_CORRUPTED_DATA	0x1B	
IOERR_CORRUPTED_RPI	0x1C	
IOERR_OUR_OF_ORDER	0x1D	Possible bad cable/link noise
IOERR_CORRUPTED_ACK	0x1E	
IOERR_DUPLICATE_FRAME	0x1F	
IOERR_INVALID_ACK	0x20	
IOERR_BAD_40BIT_ADDRESS	0x21	
IOERR_RESERVED	0x22	
IOERR_RESERVED	0x23	
IOERR_RESERVED	0x24	
IOERR_ABORT_MULTI_REQUESTED	0x25	
IOERR_RESERVED	0x26	
IOERR_RESERVED	0x27	
IOERR_LINK_BUFFER_SHORTAGE	0x28	
IOERR_RCV_XRIBUF_WAITING	0x29	

Troubleshooting Topics

General Situations

Table 18: General Situations

Situation	Resolution
Cannot See Other Host Bus Adapters (HBA)s or Host. Although HBAnyware™ is installed, only local HBAs are visible. The other HBAs and hosts in the storage area network (SAN) cannot be seen.	HBAnyware uses in-band data communication, meaning that the management server running HBAnyware must have a physical Fibre Channel (FC) connection to the SAN. All the HBAs in the SAN will be visible if: • The other servers have a FC connection to your zone of the SAN. • All other HBAs are running HBAnyware and the appropriate driver. • The other HBAs are Emulex HBAs. **Note:** HBAnyware must be running on all remote hosts that are to be discovered and managed. Remote capabilities of HBAnyware are subject to fabric zoning configuration. Remote hosts to be discovered and managed by HBAnyware must be in the same zone.
Cannot see multiple zones on the same screen of my management server running HBAnyware.	Provide a physical Fibre Channel connection into each of the zones. For each zone you want to see, connect an Emulex HBAnyware enabled port into that zone.
lputilnt Installs, but HBAnyware Does Not. When you run setupapps.exe, lputilnt installs but HBAnyware does not. You have attempted to manually install the utilities for the driver before manually installing the driver	Perform the installation tasks in the following order: 1. Install the driver (see the Installation section). 2. Install the utilities (see the Installation section). Perform the installation tasks in the following order: 1. Install the driver (see the Installation section). 2. Install the utilities (see the Installation section).
The SAN management workstation does not have a physical Fibre Channel connection into the SAN because the other management tools are all out-of-band. Can HBAnyware be run on this SAN management workstation?	From the SAN management workstation, run a terminal emulation session into one of the servers that has HBAnyware loaded on it. For Windows servers, use the operating system's terminal services option.
Cannot see new (logical unit numbers) LUNs. Although new LUNS were created on the storage array, they do not appear in HBAnyware.	Refresh the screen.
The HBAnyware Security Configurator (Security Configurator) software package will not install. An error message states that the latest version of HBAnyware must be installed first.	The system either has no HBAnyware software installed or has an older version of the HBAnyware software installed. In either case, obtain the latest version of the HBAnyware software and follow the installation instructions. Remember to install the HBAnyware software before installing the Security Configurator package.
HBAnyware appears on remote servers in the SAN.	To prevent HBAnyware from appearing on remote servers in the SAN, disable the HBAnyware service. Disabling this service or process prevents the local servers from being seen remotely.

Table 18: General Situations (Continued)

Situation	Resolution
Cannot access formerly accessible servers via the Security Configurator or the HBAnyware Utility.	This is a symptom of two different problems. • New Keys Were Generated While Servers Were Offline • Security Removed While Servers Were Offline See Table 23 on page 154 for details regarding these problems.
Cannot run the Security Configurator on a system that is configured for only secure access. You cannot run the Security Configurator on a system that is configured for only secure server access (it has no client privileges). The following message is displayed when the Security Configurator starts: “This system is not allowed client access to remote servers. This program will exit.”	You cannot run the Security Configurator on a system that is configured for only secure server access. Click **OK** to close the message and the Security Configurator stops.

Security Configurator Situations - Access Control Group (ACG)

Table 19: HBAnyware Security Configurator - Access Control Group Situations

Situation	Resolution
All servers are not displayed. When you run the Security Configurator on the Master Security Client (MSC), you do not see all of the systems in available servers or ACG Servers lists. When you run the Security Configurator on a non-MSC, you do not see all of the systems you should see in the ACG Servers list.	Make sure all of the systems are connected to the Fibre Channel network and are online when you start the Security Configurator. Discovery of the systems is done only once, at startup. Unlike the HBAnyware utility, there is no Rediscover Devices button. Therefore, the Security Configurator must be restarted to rediscover new systems.
Cannot add or remove a server. The Security Configurator shows only a list of the systems in this system's ACG. You cannot add or remove systems from the ACG.	This is normal. You can modify the ACG for your system only on the MSC or on a parent client system.
HBAnyware Utility shows non-ACG Servers. The HBAnyware utility shows servers that are part of the ACG and that are not part of the ACG.	The HBAnyware utility discovers unsecured servers as well as servers that are part of its ACG. The servers that you see that are not part of the ACG are unsecured. They will be discovered by any system running the HBAnyware utility on the same Fibre Channel fabric.

Security Configurator Situations - Access Sub-Groups (ASG)

Table 20: HBAnyware Security Configurator - Access Sub-Groups Situations

Situation	Resolution
ASG Appears to Be Non-Hierarchical. It is possible from a higher-level client (such as the MSC) to create an ASG 1 with system A as the client and systems B, C, D, and E as servers. Then create an ASG 2 with system E as the client, but with systems F and G as servers even though F and G are not part of ASG 1. This makes the topology non-hierarchical.	See “Non-Hierarchical and Hierarchical ASG” on page 155 for a discussion and a resolution to this situation.
Cannot add or remove a server.	When all of the systems in an ACG are running on a single fabric, they are all available to be added to any ASG. However, if the client is connected to more than one fabric, it is possible that not all of the servers in the client's ACG are physically accessible by a chosen client for an ASG. In this case, those servers are not available to be added to that ASG. If you add a system to an ASG as a server, and then make the system a client to a child ASG, you cannot remove it from the ACG it belongs to as a server until you delete the ASG that it is a client to. Before you delete a server from an ASG, you must first remove the server from any lower level ASGs to which it belongs.
In the ASG tree of the Access Sub-Groups tab, one or more of the names of the ASGs is displayed as "- ASG (Client Offline) -"	The client system for the ASG was not discovered when the Security Configurator was started. This is a symptom of two different problems. • All Servers Are Not Displayed • New Keys Were Generated While Servers Were Offline See Table 23 on page 154 for details regarding these problems.
Not All Servers are available to an ASG. When you create a new ASG or modify an existing ASG, not all of the servers in the ACG are available to be added to the ASG.	A client system can be connected to more than one fabric. While the system the Security Configurator is running on may be able to access all of the servers in its ACG, it is not necessarily the case that the selected client for the ASG can access all of the servers. Only those that can be accessed by the selected server will be available.

Security Configurator Situations - Backup Masters

Table 21: HBAnyware Security Configurator - Backup Masters Situations

Situation	Resolution
Cannot create a backup master.	Select a system (or group of systems) from the MSC to be the Backup Master. The system must be either an unsecured system (which will be secured by being made a Backup Master), or a system that is not part of any ASG (client or server). These systems will mirror the MSC's security configuration. Because the Backup Master may some day take over as the MSC, the Backup Master must be able to physically access all of the systems that the MSC can access. Therefore, if the MSC is connected to multiple fabrics, the Backup Master also must be connected to those same fabrics. When you select a Backup Master, the Security Configurator displays a warning if it detects that the system selected to be a Backup Master is not able to physically access the same systems that the MSC can access
Cannot modify the Security Configurator.	Select a system (or group of systems) from the MSC to be the Backup Master. The system must be either an unsecured system (which will be secured by being made a Backup Master), or a system that is not part of any ASG (client or server). These systems will mirror the MSC's security configuration. The Backup Master has client access from the HBAnyware utility to all of the servers in the MSC's ACG. However, the Backup Master does not have client access to the MSC and it cannot modify the security configuration (create, modify or delete ASGs).
No Backup Master and the MSC Is no longer available. You do not have a Backup Master and the MSC system is no longer available. The servers are still secure. You installed the Security Configurator on another system, but cannot access those servers to remove the security from them.	The servers are no longer part of a valid security configuration because there is no MSC to provide master control of the configuration. In order to reset the security on the affected servers, you must contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they should be seen by the Security Configurator and the HBAnyware utility. At this point, you can set up security again through another MSC. At this time, also create a Backup Master.
The Backup Master tab is not available.	The **Backup Master** tab is displayed only when the Security Configurator is running on the MSC or a Backup Master. You use this tab to set up a system or systems to be backups to the MSC and to replace the MSC with a Backup Master. Each time you start the Security Configurator on the MSC and there is no Backup Master assigned, a warning message urges you to assign at least one Backup Master to prevent the loss of security information if the MSC were to become disabled.

Security Configurator Situations - Error Messages

Table 22: Error Message Situations

Situation	Resolution
The following error message is displayed when creating an ASG: “The Access Sub-Group name already exists. Please use a different name.”	You entered a duplicate ASG name in the Access Sub-Group Name field. At each level of the security topology, each ASG name must be unique. Click **OK** on the message and enter a unique ASG name.
The following error message is displayed when deleting an ASG: “The Access Sub-Group parent’s ASG is offline. You should delete the ASG when the parent ASG is available. This ASG should only be deleted if the parent ASG will not be available again. Are you sure you want to delete this ASG?”	The offline ASG entry serves as a placeholder for where the real ASG would be in the tree. You can neither modify nor delete it (although it is removed from the display if all of the child ASGs are deleted). It is possible to delete the child ASGs of the offline ASG. However, it is recommended that you delete them only if the client for the offline ASG will never be put online again. It is best to delete child ASGs when the parent ASG is online. Click **Yes** on the error message to delete the ASG or No to close the message without deleting.
The following error message is displayed when starting the Security Configurator: “This system is not allowed client access to remote servers. This program will exit.”	The system you are running the Security Configurator on is already under the security umbrella as a server to one or more clients. To make this server a client (so that it can successfully run the Security Configurator), click **OK** to close the message and exit the program, then: 1. Run the Security Configurator on the MSC or on any client that has this server in its ASG. 2. Make this server a client to a group of servers.
The following error message is displayed when starting the Security Configurator: "There are no Backup Master Client Systems assigned to this security configuration. At least one should be assigned to avoid loss of the security configuration should the Master Client System become disabled."	Use the Backup Master tab to assign a Backup Master for the MSC.
The first time the Security Configurator is started in an unsecure environment, the following message is displayed: “This utility is running on an unsecure system. Continuing will allow you to set up a new security configuration making this system the Master Client System.”	Click **OK** on the message and complete the ACG setup. The system on which the Security Configurator is running will become the MSC.
When you start the Security Configurator on a Backup Master system, the following message is displayed: “Warning: This system is a backup master client system. Therefore you will only be able to view the security configuration. To make changes, you must run this utility on the master client system.”	Because each Backup Master system receives all the updates that the MSC makes to the security configuration, the Backup Master systems must be online when the Security Configurator is running on the MSC. Otherwise, updates to the security configuration are not reflected to the Backup Master. If the Backup Master becomes the MSC, corruption of the security configuration may occur. Click **OK** to close the message.

Security Configurator Situations - Master Security Client (MSC)

Table 23: Master Security Client Situations

Situation	Resolution
The MSC is no longer bootable or able to connect to the FC network.	You must reassign a Backup Master as the new MSC from the Backup Master. **Warning:** Use this procedure only if the MSC cannot relinquish control to a Backup Master. For example, if the MSC is no longer bootable or able to connect to the FC network. Under any other circumstances, if the Backup Master takes over as the MSC and the MSC is still running or comes back online later, there will be two MSCs for the same security configuration. This will eventually lead to corruption of the security configuration.
New Keys Were Generated While Servers Were Offline. A "Generate New Keys" operation was performed while one or more of the servers were offline. Now those servers can no longer access the Security Configurator or the HBAnyware utility.	The servers are no longer part of the security configuration. In order to reset the security on the affected servers, you must contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they can be added back into the security topology by the MSC. **Note:** If the server was also a client to an ASG, then when you run the Security Configurator on the MSC or a parent client of this client, its label in the ASG tree of the Access Sub-Group tab will be "-ASG (Offline Client) -". You must delete the ASG (after deleting the child ASGs) and recreate the ASG configuration of this client and its child ASGs.
Security Removed While Servers Were Offline. Security was removed while one or more servers were offline. You can no longer access those servers from the Security Configurator or the HBAnyware utility.	The servers are no longer part of the security configuration. In order to reset the security on the affected servers, contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they should be seen by the Security Configurator or the HBAnyware utility.

Non-Hierarchical and Hierarchical ASG

It is possible from a higher-level client (such as the MSC) to create an ASG 1 with system A as the client and systems B, C, D, and E as servers. Then create an ASG 2 with system E as the client, but with systems F and G as servers even though F and G are not part of ASG 1. This makes the topology non-hierarchical (see Figure 77).

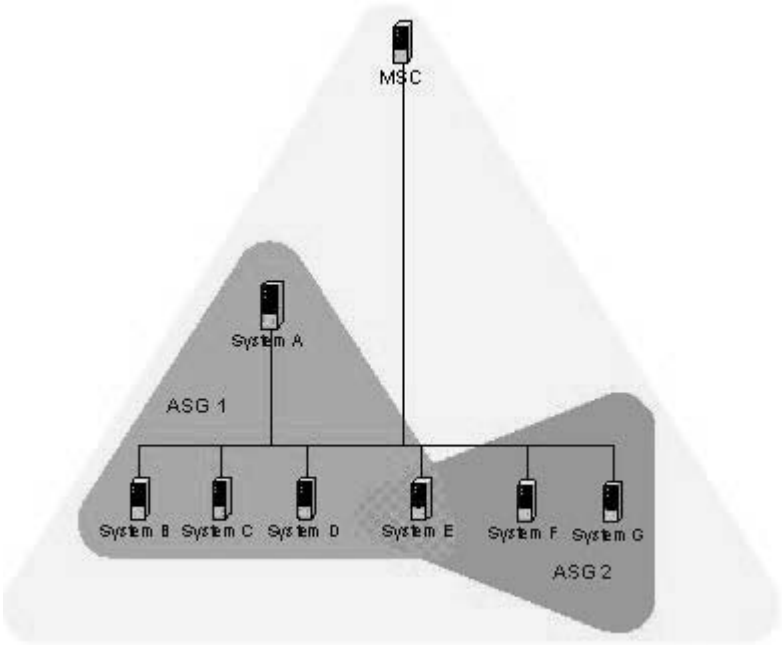

Figure 77: Non-hierarchical ASG Scenario

System E is part of ASG 1, but has been made a client of ASG 2, and both of the servers in ASG 2 are not part of ASG 1. You could not create this ASG on system A, but you could on the MSC (or on a parent client) because it can access systems F and G. Although not shown in the picture, it is also possible to make system A a server in ASG 2, creating a case where system A and system E are both clients and servers to/of each other.

While the Security Configurator will allow you to set up ASGs this way, it is best not to create a topology like this as it can lead to confusion. The best way is to set up the ASG on the MSC (or a higher-level parent) where the clients and servers do not cross over into other ASGs. Then set up ASGs on clients of those ASGs in the same manner, keeping the topology hierarchical (see Figure 78).

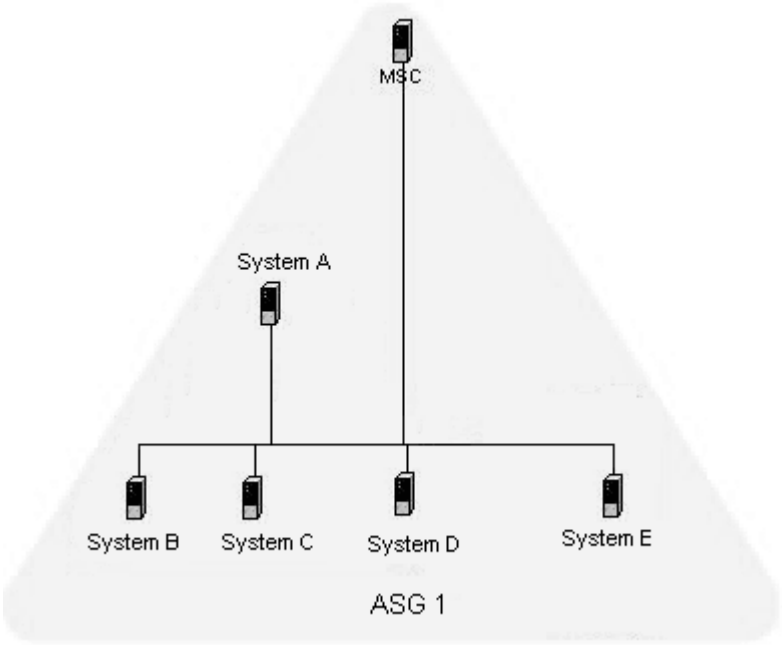

Figure 78: Hierarchical ASG Scenario